ESPRIT Project 27028 : electronic commerce legal issues platfrom : deliverable 1.2. : analysis of the RTD projects assisted

Dusollier, Séverine

Publication date:
1999

Document Version
Publisher's PDF, also known as Version of record

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

Deliverable 1.2. - Analysis of the RTD projects assisted

CRID - Séverine DUSOLLIER

24 January 1998

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

Deliverable 1.2. - Analysis of the RTD projects assisted

CRID - Séverine DUSOLLIER

24 January 1998

Content

1. Introduction

The aim of this deliverable is to provide an overview of the assistance to other EC-funded projects carried out so far by ECLIP.

The task of assistance is the core of the E-CLIP Project. Therefore, a particular attention has been devoted thereto in the last months, as it will be explained hereinafter.

Such assistance namely consists of :

- identifying the legal issues raised by the RTD projects developing an electronic commerce initiative
- providing these projects with ongoing legal advice relating in particular to the specific field(s) of law and geographical area(s) concerned.
- ensuring a proof-reading of contracts, general conditions or other relevant documents submitted by these projects while not being a substitute to services from professional lawyers and advisers
- disseminating within the E-CLIP platform (to the partners and to others assisted projects) the public information from the RTD projects assisted on the solutions they develop.
- inviting participation in workshops organised by the E-CLIP partners, which are aimed both at providing information on the legal issues of electronic commerce and to disseminate the relevant technology developments that could facilitate the compliance of electronic transactions with the law.

2. Process of Assistance in E-CLIP

At the beginning of ECLIP, a presentation of our project and of the scope and type of assistance we could ensure, has been disseminated to around twenty new Esprit funded projects.

Other projects have been approached during European conferences in which the ECLIP project has been the object of a lecture, or during clustering activities organised by the Commission or by the ESPRIT project EC-CLUSTER. Other projects have heard about ECLIP through our Website.

The projects seeking assistance contact the CRID that is in charge of the co-ordination of ECLIP assistance. The CRID submits them a questionnaire to assess the type of interest and possibility for E-CLIP to answer the demand. This questionnaire addresses a short description of their projects, examination of their needs for and acceptance of legal assistance, assessment of the supplementary resources and costs for taking that assistance into account. Once the completed questionnaire is received, it is analysed with other questionnaires to identify the profiles and ways of assistance demanded and their feasibility.

A first meeting between the project seeking assistance and the ECLIP partners normally takes place so as to present the project and to give a first overview of the relevant legal aspects to be considered.

On the basis of this meeting , the scope of assistance can be agreed with the project (tasks, time schedule, E-CLIP partner(s) providers, resources considered, etc.). Usually, this agreement is made also by written in order to commit the project we will assist.

This is the model of agreement we conclude :

Agreement

In the frame of the ECLIP assistance to X, ECLIP partners will provide co-ordinator of X with the following services free of charge, under the following conditions:

Tasks and number of man-days per partner

During the period of ECLIP assistance, X will address a two-monthly progress report (1 page) to BvD and CRID related to any issue affecting the assistance in order that contact is adequately maintained between the providers of assistance and the receiver.

The assisted projects receive automatically all the legal surveys drafted by ECLIP and are invited to the workshops we organise either to present their project, either to attend.

3. Scope of the assistance

It has been decided to leave out of assistance the projects which request assistance on matters outside the actual scope of electronic commerce, such as for instance IPR issues linked to the exploitation of their project or the analysis of specific legislation whose application appears not being different in an e-commerce environment than in a traditional one, e.g. the transportation and travel agencies regulations.

Another problem is also that some projects that will face certain legal problems related to e-commerce not in the project phase but in the exploitation phase, when they want to commercialise their product. For commercialisation especially taxation and electronic payment issues are getting more important. But ECLIP can only grant assistance in the actual project phase.

Moreover, the scope of the assistance on legal issues that can be provided by ECLIP partners largely depends on the level of clarity of the project to be assisted. Either the needs or the legal problems are clearly defined by the project. In this case, precise tasks of assistance can be agreed upon at the outset. It was namely the case for AIMEDIA, TRIP, COSMOS, TELEPOLIS and FACTMERCHANT which were aware of some of the legal constraints.

Either, the needs are not clear and the project lacks of a certain awareness of the legal constraints its development might encounter. In this case, a first task of assistance consists of ensuring a sort of legal 'audit' of the project so as to scan the legal pitfalls and issues raised by the system or services developed and offered by the project. This audit has also the objective to enhance a further need for assistance. This has namely been done for Internet Megastore and TRADE as a basis for further assistance.

4. Assistance carried out so far

4.1. AIMEDIA

4.1.1.Scope of the project

The general objective of AIMEDIA is to develop a commercial integrated intelligent agent for targeted advertising. Two pilot applications are scheduled : one with OTTO VERSAND, a German distant selling company, the other with SAINSBURY, a UK supermarket launching a service on-line.

4.1.2.Needs for assistance

A first and clear demand from AIMEDIA was focused on privacy issues since the project will have to collect and process a great number of data related to individuals such as profiling data. AIMEDIA had a great concern on that point and were pretty aware of the implications of privacy legislation for the project. They were also concerned by the so-called privacy-enhancing technologies for which ECLIP was able to provide them with an overview of the legal consequences of the utilisation of such PET's. The system namely to be used by AIMEDIA is the platform P3P. Therefore, it was agreed to carry out a study on the consequences of the integration of P3P from a privacy point of view.

Another demand was on advertisements regulations since the goal of the data mining and user profiling carried out by AIMEDIA is to ensure a targeted advertisement.

Finally, E-CLIP and AIMEDIA have agreed on the following workplan :

-Task 1 : drafting the part 'Legal Constraints' in the deliverable 13 of AIMEDIA.

It consists of providing an overall overview of the legal aspects of electronic commerce relevant to AIMEDIA project. The practical issues raised by the project should be addressed. The legislations to be covered are the common European framework and, when it differs from this common rules, the UK and German laws (place of business of both pilots).

ECLIP Partners involved :

CRID : Data Protection & Advertisements regulations ,UIB : Digital signature ,NRCCL : International private Law

Task 2 : Reviewing the other parts of Deliverable 13 released by AIMEDIA

ECLIP Partners involved : CRID, UIB & NRCCL

Task 3 : Reviewing the Privacy-enhancing technologies envisaged to be implemented in AIMEDIA tool, such as P3P.

ECLIP Partners involved : CRID

Task 4 : Reviewing the 'Marketing Strategy' developed by AIMEDIA for the pilot applications & helping the legal design of the pilot applications (which will start on January 1999).

ECLIP Partners involved : CRID, UIB ,NRCCL

4.1.3.Assistance provided

E-CLIP has drafted an important part of the AIMEDIA deliverable 13 on the legal constraints and particularly on privacy and advertisement regulation (ANNEX 1).

On advertising regulations the following points have been addressed :

⇒ to what extent the advertiser is bound by the content of advertising

⇒ the difference between an advertising and an offer

⇒ the consequences of the type of medium (on-screen, e-mail)

⇒ the information to be provided to the consumer

⇒ the right of a consumer facing advertising and marketing practices

⇒ legal rules applicable at European, Germany and United Kingdom level, namely the misleading and comparative advertising directive, the Green Paper on commercial communications.

From a privacy point of view, an identification of the personal data likely to be collected and processed in the AIMEDIA scenario as the controller thereof has been made. Afterwards, the principles of data protection were laid down and recommendation for integrating the compliance of those principles in the AIMEDIA applications were drawn. Finally the rights of data subjects and the obligations and duties imposed on controllers have been examined. A particular attention has been paid to the German data protection principles laid down in the multimedia law since one AIMEDIA application will occur in Germany.

A further analysis of the digital signature (ANNEX 2) and the relevant issues of applicable law (ANNEX 3) were added later on , since they were not ready to be integrated in the deliverable 13.

The contents of the international private law contribution are the following :

- an introduction to IPL principles and issues
- the determination of the competent jurisdiction in the field of contract and tort for data protection issues
- the determination of competent jurisdiction in legal disputes relating to advertisements regulations
- the law applicable to data protection issues. Three questions have been addressed her :
  - the situation where the controller has different places of establishment
  - the question as whether the data mining can be considered as a contract between the data subject and the controller

- the applicability of rules of ordre public to data mining

- the law applicable to advertising

- the law applicable to liability on the basis of loss suffered due to misleading information

A review of the deliverable 13 has also been carried out by ECLIP, particularly on the PET's developments and other technical aspects relevant from a privacy point of view.

4.1.4.Follow-up of the assistance

The two surveys on privacy and advertisement issues have been presented to the AIMEDIA consortium and have caught the interest of the partners. Design conclusions , especially in terms of technical requirements and on user interface were drawn and integrated in the over-all framework design of AIMEDIA software. Namely, the following requirements have been integrated :

- a clear message on privacy matters is sent to the users when offering AIMEDIA agents

- when data are collected through a questionnaire, the purpose of this collect and processing of data is explained to the users.

- AIMEDIA will insist on the responsibility of the retailers to ensure the technical and organisational protection of data through security policies.

- AIMEDIA will define a clear access right policy

- The user interface developed in the project will integrate a profile manager enabling the user to keep control of his profile by way of technique of opting in and opting out.

- An explicit consent of the data subject will be asked for the possibility to share the user profiling between several retailers.

A publication is currently being drafted jointly by AIMEDIA and CRID on the privacy and advertising issues of the AIMEDIA project as a case study.

4.1.5.Further Assistance foreseen

The tasks 3 and 4, as mentioned in point 4.1.2. will be carried out in the next weeks. They will consist of reviewing the relevant deliverables of AIMEDIA. Those deliverables have not been transmitted to ECLIP yet. Conformance of technical specifications, in particular the user interface design, to legislation constraints should be checked. Awareness on evolving standards , such as OPS and P3P, could also be continued.

4.2. TRADE

4.2.1.Scope of the TRADE project

TRADE will operate three trials of Electronic Commerce (EC) in Italy and Spain with multiple EC applications in the following market sectors:

reservation and sales of tickets for entertainment events (Business to Consumer and Business to Business),

* co-operative working in the fashion sector (B-B),

* provision of legal and administrative services (B-C and B-B)

The trials in Italy and Spain will be deployed in the context of the respective National Hosts. Based on the first trial results, TRADE will assess the adopted technical solutions and user acceptance, which will guide the anticipated improvements and extensions of the subsequent trials. Legal & Normative constraints to EC deployment in Europe will be studied.

The main objectives of the project are :

* integrate, test and operate in the context of trials, over broad band extensions of the Internet,

* secure multimedia EC platforms for residential and business users adopting, as far as possible, existing or emerging technologies and products based on open standards;

* experiment and provide security mechanisms suited for access to EC services and coupled with secure processing of electronic payment transactions based on consolidated and emerging standards;

4.2.2.Needs for assistance

The needs of TRADE partners were not really defined. They request an assistance particularly in the applications they will develop. At the same time, ECLIP has managed to point out that the legal issues specific to the involvement of the TRADE server itself in all applications should be considered as well. Therefore, a first task has been to carry out a legal audit of the TRADE project.

The following tasks have been agreed upon :

Task 1 : Review the deliverable 5 & 7 of TRADE on pilot application. This task consisted of considering the legal issues of the envisaged trials.

ECLIP partners involved : CRID, ITM, QMW, UIB, NRCCL

Task 2 : Considering the possible legal issues of the TRADE platform

ECLIP partner involved : CRID

4.2.3. Assistance carried out

The two tasks hereabove have been the object of one consolidated report (ANNEX 4).

The first part of this paper from ECLIP is limited to an overall consideration of the legal issues arising in the pilot applications developed in the project TRADE. Two Pilot applications have been reviewed by E-CLIP partners on the basis of the deliverable 5 and 7: on one hand the so-called "ticketing scenario" which sets up an on-line broker systems for reservation and provision of tickets for cultural and sports events, on the other hand the so-called "administrative and legal scenario" which sets up a service for providing administrative and legal services on-line. The following issues have been considered :

- the regulatory framework of digital signature
- the IPR issues arising from the use of protected material, the multimedia catalogue developed in the ticketing scenario and the protection of website
- the application of data protection legislation to both applications
- an overview of the distance selling directive
- the problems of advertising regulations relevant for the ticketing scenario
- the electronic payment issues
- the issue of transfer pricing for a taxation point of view in the administrative and legal application
- accounting problems raised by the electronic catalogue developed in the ticketing scenario
- the determination of VAT, particularly in the ticketing scenario
- the question as to whether some actors in the ticketing scenario may be considered as on-line intermediaries and the liability consequences thereof
- identification of contractual liability issues
- a first overview of the applicable law to contract obligations, consumer protection, copyright infringement, liability for misleading information and security requirements.

The second part addresses the legal issues raised by the development and operation of the TRADE server in itself. It covers :

- an analysis of the nature of the TRADE server
- legal issues raised by the technical solutions adopted and integrated in the TRADE server, such as access control mechanisms (digital signature and cryptography, data protection legal protection of conditional access systems), payment gateway, anonymisation gateways (data protection issues), Microsoft Transaction Server (from calculation of sales tax to calculation of VAT, consumer protection)
- consequences of the TRADE server in applicable law to applications.

4.2.4.Follow-up of the assistance

We don't know to what extent the legal recommendations made by E-CLIP have been integrated in the TRADE project.

Other needs for legal assistance should be defined by the legal partner in TRADE project on the basis of the ECLIP deliverable on legal issues and on the outcome of the first task of assistance.

4.2.5.Specific Issues

The TRADE project is a large project, sometimes not clearly defined, which develops and sets up at least three different pilot applications. Legal issues might be really different for each application which implies a need for three different assistance, to which should be added the assistance for the TRADE platform itself. Besides, it was not clear for the TRADE partners that the development of common infrastructure and server would entail specific legal constraints. Therefore, we could limit this assistance to some parts of TRADE development either to the TRADE server, either to one or two pilot applications

4.3. TRIP

4.3.1.Scope of the TRIP project

TRIP (Travel Reservation and Interactive Purchase) aims to deliver a working electronic commerce infrastructure for the European Travel market to the benefit of Travel Agents, SME leisure operators and their customers. A consortium of seven companies from the UK, Italy, France and Portugal are involved in the project. The pilot will be conducted in these countries and business plans for the distribution of the TRIP platform across Europe form an important part of the project.

4.3.2.Specific Needs for assistance

The co-ordinator of TRIP, Mrs Susan Powell had already defined some precise legal questions on which she requests assistance. This has greatly facilitated the intervention of ECLIP and made it more rapid.

The questions concerned more or less the following matters (details of the questions in ANNEX 5) :

1. Applicable laws
2. regulatory framework of Travel business
3. legal issues of the Euro
4. Liability for payments
5. Data protection and liability
6. Calculation of VAT
7. IPR issues, e.g. Protection of system name, Protection of the TRIP system and software, Registration of Web Site(s) and Domain Names, Copyright in TRIP Data / information, copyright in a Web Site, Hyperlinks and Gophers

8. electronic contracting

9. Liability for advertisements on the site.

10. Prevention of fraudulent, defamatory or obscene material from the TRIP Operator

4.3.3.Assistance carried out

A first set of answers to the questions above have been transmitted to TRIP on the 23d of December (ANNEX 6). This covers some questions in taxation, IPR, a first overview of IPL issues and of privacy questions.

A second set of answers has been sent by the end of January. (see ANNEX 7)

4.3.4.Specific Issues

Some questions are outside the scope of ECLIP, either because they are too specific to the travel sector and infer from specific regulations, either because they are not specifically linked to electronic commerce development (such as questions about EURO).

Therefore, we have let some TRIP questions out of our intervention.

4.4. COSMOS

4.4.1. Scope of the COSMOS Project

The COSMOS project aims to develop a support platform for *business transactions* across the Internet based on a generic **contracting service**. Potential users of such a system include small and medium enterprises and even individual persons. The contracting service enables its users to negotiate, sign, and settle electronic contracts across the Internet without leaving a uniform and flexible system environment.

The main objectives of the project are the following :

Analysis of legal and organisations requirements & constraints

Architecture for the contracting service

Preparation of a suite of software components for contracting support

4.4.2.Specific Needs for assistance

The key question for COSMOS is contract law issues. Therefore, COSMOS works closely with UIB, in charge of contractual matters in ECLIP.
Some questions about contract law and certification have been raised by COSMOS, as follows:

1. *Which levels of certificate contents do you consider to be required for the COSMOS application (corresponding to the 4 levels of Verisign certificates)?*
2. *Which do you expect (or would you suggest) to be standardised?*
3. *How is the verification of representatives handled today in the classical way and electronically? Which solution would you propose to handle this electronically?*
4. *What is the current practise/standardisation/which would be the ideal situation for that handling of revocations of power-of-attorney certificates?*

5. *Our Contract Model: We designed an object model for contracts containing parties, obligations, roles, etc. as semantic concepts. We would like to have this approved by some legal experts concerning - terminology - correctness of the model. This model requires some explanations if the reader is not familiar with object-oriented modeling techniques, therefore I consider it better to discuss this "face-to-face".*
6. *Compound Contracts: In our model we assume that a set of contracts may be signed as a whole in one single transaction (example: The COSMOS contract between the consortium and the EU and the Consortium Agreement). We would like to build a system that enables the users (i.e., the contracting parties) to sign this bundle of contract at once. However, each party's signature will be interpreted as to apply only for those contracts in which the respective party is involved.*
7. *To which extend is it possible to supersede different (national) legal frameworks by a framework contract between market participants and the contracting service provider? What we would like to have and the end here is a Terms-and-Conditions document that suits for the provider of the COSMOS contracting service.*
8. *Is there a concrete comparison of national contracting legislation throughout the EU available, especially one that concerns online contracting?*
9. *Role of notary in COSMOS We will build a software component that acts as an electronic notary by providing the following services as atrusted party:*
10. *verifying the proxy regulations for all contract parties (who is authorised as a sigantory, handling of power-of-attorney-documents, etc.)*
11. *countersigning of signatures for a contract document*
12. *archiving the contract document, the parties' signatures and its own*
13. *which organisational/legal requirements need to be satisfied in order to deploy an electronic notary. Please don't understand notary in the restrictive definition of the notary public, but rather as a trusted third party (a Bank, a CA) that provides this service.*
14. *For supporting a contracting service at an international (at least EU) level, we need some input on the roadmap for harmonization in the following fields:*
15. *electronic signature legislation*
16. *the definition, role and development of electronic notary services*
17. *Finally, we need in-depth knowledge on how contracts are modeled according to the different legal frameworks in the EU countries. Today we assume the German law for the COSMOS system, but we are interested if there are maybe confliction perceptions in these countries how a contract is modeled.*

Other planned tasks of assistance are the following :

Task 1 : Review of requirement report

ECLIP Partners involved : CRID, ITM, NRCCL, UIB , QMW

Task 2 :Proposals for compound contracts

CRID, NRCCL , UIB

Task 3 Research on taxation issues

ECLIP Partners involved : ITM

Task4. Further practical support on questions about digital signature and Contract law

ECLIP Partners involved : UIB, NRCCL

4.4.3.Assistance carried out

The first task has been carried out so far (ANNEX 8). Besides, UIB has worked on contract law issues directly with COSMOS co-ordinator, namely on the questions raised above.

COSMOS has also asked to present the contracting service it develops at the next workshop on contract law issues in Palma which could serve as a forum for discussion for the application on the ECLIP thinking on electronic contracting.

4.5. INTERNET MEGASTORE

4.5.1.Scope of INTERNET MEGASTORE project

Internet Megastore aims at applying new technologies to the exchange of goods and services, allowing small shops (outlet) to carry out their transactions through an "intermediary" created

for such purpose. We are in front of a "virtual commercial center and different stores that use a space within such virtual center, where they offer their goods and services.

The project is focused on consumer merchandising and on the way chains of retailing stores may use Internet to extend their line of business to home shopping. In this scope it is important to make a distinction of the double way of proceeding which generate two different kind of regulation, one for the relation between Internet Megastore and consumers (through Internet), and another for the relation between Internet Megastore and small shops (through Internet or by other ways).

This project studies and tries to implement a solution for electronic consumer merchandising that most closely meets the requirements of both consumer and retailers. The project end result will be to build a virtual outlet.

4.5.2.Specific needs

This project presents the same lack of clarity as TRADE. Therefore, the assistance of ECLIP has been limited at present to outline the relevant legal issues that might be raised by the development of the project. Further assistance should be agreed upon that basis and precise needs and tasks are to be defined.

4.5.3.Assistance carried out

A first 'audit' report on the legal issues of INTERNET MEGASTORE (ANNEX 9) has covered the following points :

- VAT treatment of services offered by INTERNET MEGASTORE
- collection of tax and information by intermediaries
- IPR issues raised by the presentation of products
- protection of the INTERNET MEGASTORE website
- trademark issues

- contractual, security and data protection issues raised by electronic payments
- application of data protection principles to INTERNET MEGASTORE
- legal issues of promotional information and commercial communication
- analysis of the distance selling directive
- distinction between offer and acceptance
- analysis of the unfair term directive
- time and place of the conclusion of contract
- evidence and authentification

4.6. PETER

4.6.1.Scope of the PETER project

The project sets up a training courseware and consultancy documents on the Intellectual Property Rights in electronic commerce for SMEs. It will also develop software solutions. The training is aimed at providing SMEs with a technical and legal overview on the electronic commerce and the IPR framework.

4.6.2.Specific Needs for assistance

The copyright collective society ALCS is one partner in the PETER project and is in charge of providing the content of the training courseware on the copyright and legal framework. But this content is limited so far to a common law point of view. Since PETER aims at providing training in whole Europe, they want us to help them draft a more continental approach.

Therefore we have agreed on the following tasks :

-Task 1 : drafting the content of the training package developed by PETER

It consists of adding to the existing training package the legal IPR framework of other EU countries than UK and Ireland. This will be carried out in collaboration with ALCS, provider of legal information in PETER.

ECLIP Partner Involved: ITM with the assistance of other ECLIP partners if needed

Task 2 : Reviewing the training packages released by PETER

ECLIP Partners involved : CRID, UIB, ITM, QMC & NRCCL

4.6.3.Specific Issues

PETER is strongly oriented towards a commercial exploitation of their training courseware. Therefore, the question of the rights in the content provided by ECLIP has been raised. Without being an issue, this is a particular characteristic of this assistance which could lead to a participation of ECLIP in the exploitation of another project.

4.7. FACTMERCHANT

4.7.1.Scope of the FACTMERCHANT Project

The overall purpose of FactMerchant is to exploit existing technologies and protocols to demonstrate and promote the use of an integrated Electronic Commerce platform for searching, browsing and manipulating business and financial information on the Web. Its goal is to provide a cost effective and easy to use solution of interest to European Small and Medium Sized Enterprises (SMEs). FactMerchant will provide access to branded business and financial information, including financial and credit analysis, market and broker research, real-time news and delayed financial rate information. Electronic Commerce offers significant attractions to European companies, particularly in peripheral regions of the European Union.

4.7.2.Specific needs for assistance

The project has already examined deeply some legal issues and there is no need for further involvement of ECLIP in these areas. This is namely the case in privacy and cryptography, both topics on which Factmerchant has written extensively.

ECLIP should intervene for reviewing agreements entered between on the one hand Factmerchant and the suppliers of information, and on the other hand, Factmerchant and customers.

Other fields of interest are liability for inaccurate information and copyright infringement since Factmerchant will be a host intermediary.

Legal issues of invoice are also relevant as Factmerchant will develop an automated invoice, as well as other relevant taxation issues (taxation of royalties).

Factmerchant has also showed interest in Electronic Rights Management Systems.

Finally, E-CLIP and Factmerchant have agreed on the following workplan :

- *Task 1 : Review the draft agreements prepared by Factmerchant.*

  ECLIP Partners involved : CRID (mainly liability clause and privacy), ITM (mainly copyright clause), UIB , NRCCL , QMW

- *Task 2. Overview of liability issues involved in Factmerchant, particularly for inaccurate information and for copyright infringement.*

  ECLIP Partner involved: CRID

- *Task 3. Legal aspects of invoice system : legal and administrative requirements, electronic payments, VAT issues, evidence issues and digital signature*

  ECLIP partners involved : ITM , QMW , UIB if needed for digital signature and evidence aspects

- *Task 4 : overview of the taxation of royalties*

  ECLIP Partners involved : ITM

- *Task 5 : information on Electronic Copyright Management Systems* :

  ECLIP Partners involved : ITM, CRID

4.7.3.Specific issues

The FACTMERCHANT project is coming to an end by the end of March 1999. Even if the project can rely on a further 3 months extension, it implies that the intervention of ECLIP arrives late in the course of the project.

A consequence thereof is that our assistance might be limited to some extent, since some issues have already been considered and maybe solved by FACTMERCHANT. Furthermore, the outcome of our assistance might be integrated no sooner than in the exploitation phase of FACTMERCHANT.

4.8. CYBERBRAND

4.8.1.Scope of the CYBERBRAND project

The aim of this project is the sales controlling of retail products. It intends to help online-vendors optimise the image of their products on the Internet, and use the results as success factors for implementation of new strategies. The main goal in the project is to offer a system, which enables the creation and the controlling of brand products, which will be sold directly via the Internet.

Through CYBERBRAND, a company will be able to communicate different images of their brands. The company can target several different market segments or niches simultaneously without changing their physical offer.

The main objectives of the project are the following :

- An IT-solution developed as a Toolkit which is bundled to marketing and on-line agencies
- Two pilot applications, one in Germany and one in Italy, will be carried out
- Business plan describing the market and determine the pilot user, and which defines the marketing mix for each IT provider of CYBERBRAND.

4.8.2.Specific needs for assistance

The legal assistance is mainly expected in the field of privacy, since personal data will be used, and in the field of international private law (IPL).

Assistance in the field of privacy is needed at both European and German levels, since the project is located in Germany.

It is agreed that the assistance will be divided into two parts:

- a first one devoted to a general information disclosed on privacy and IPL issues,

- a second one where more specific assistance will be provided according to the needs of the project and its practical enforcement (for instance consumer protection issues with regard to targeted advertising if the data are intended to be used for individual commercial communications).

4.8.3. Assistance carried out

Assistance has started in January 1999. so far a first paper on the data protection implications has been carried out (see Annex 10). Other tasks of assistance are planned for the next weeks.

4.9. MEDICOM

4.9.1. Scope of the MEDICOM project

The aim of the project is to build a selling communication platform (e-commerce site) for medical equipment by developing :

1. HyperMedia Catalogue:
   - an Online catalogue with products description, announcements, advertising and price list
   - direct order process on the Internet will be possible. Orders and

	delivery forms in electronic format will be available too
	• an online library as well as documents and magazines in electronic format about medical topics and products
2. Virtual Medical Exhibition	• For expensive and specific equipment
	• Online-Test and –evaluation of medical apparatus will be possible
3. Post-Market Surveillance	• Official evaluation and communication of security and quality issues for medical equipment

4.9.2.Specific needs for assistance

A lot of legal issues are involved in the project: electronic payment, contract law, private international law, taxation, copyright, contractual liability and extra-contractual liability, privacy. It has been agreed to start the assistance by providing MEDICOM with a general overview of those issues related to this project.

4.9.3.Assistance carried out

Assistance has started in January 1999. Therefore, tasks of assistance are planned for the next weeks.

4.10. NECTAR

4.10.1. Scope of the NECTAR project

The project objective is to develop a Virtual Shop system for Retail, which will exploit the pioneering technology of Intelligent Agents to improve and personalise the interaction with the Customer.

A Business Process Reorganization activity will be performed in order to provide the Retailers with processes adapted to the innovative commercial channel.

The NECTAR system will be composed of several software modules:

- a back-end module to interface the existing Information System of the Retailer with the Virtual Shop module;

- a Virtual Shop, which maintains a data base of products and drives the commercial offer;

- a front-end built on Intelligent Agents: they will drive the interaction between the Customer and the system, taking into account preferences, habits and trends.

A pilot system will be running at mid-project, so as to measure user acceptance and to improve and adjust features and functionalities of the final system, to be delivered at project end.

4.10.2. Specific needs for assistance

It was stated that assistance is mostly needed in the fields of consumer protection, data protection, copyright issues (mainly concerning trademark and competition issues) contract law and electronic payments.

The researchers and NECTAR identified the tasks to be carried out. These are divided into two tasks:

Task 1: General information on subjects: Data protection, Consumer protection, Copyright, Contract law, and Electronic payment

ECLIP Partners involved : CRID ITM, QMW, UIB, NRCCL

Task 2: Specific assistance according to the needs of the project and its practical enforcement (to be defined later on).

These tasks are planned to take place in the next months.

4.11. TELEPOLIS

4.11.1. Scope of the Project

TELEPOLIS is a Project funded by the TEN TELECOM Program. Its objectives are the following :

Develop an electronic agent for automatic calculation of VAT and electronic invoicing (CD ROM to be commercialised in April 1999)

Develop an Interchance Platform for exchanging data necessary for automatic invoicing and accounting (with XML Technology)

.

Develop a proxy billing service for reinvoicing system

4.11.2. Specific Needs for assistance

Main issues for TELEPOLIS are on IPR protection of their software and database and on Taxation matters, even if for this field, they are working with a specialised lawyer. Three meetings with TELEPOLIS have already taken place since it seemed useful to work separately on the tax engine embedded in the CD ROM on one hand and on the Interchange Platform on the other hand.

The following tasks have been decided so far :

Task 1 : Audit of the technology developed from a data protection point of view

ECLIP Partner involved : CRID

Task 2: Analysis of the regulatory framework for Liability Disclaimer

ECLIP Partner involved : CRID

Task 3 : Protection of software and protection of integrated technologies (by patent or other means)

ECLIP Partner involved : ITM

Task 4 : Liability for mistake in VAT calculation by electronic agent

ECLIP Partner involved : CRID, ITM

Task 5: Legal requirements of invoice

ECLIP Partner involved : ITM

4.12. Overall overview of the assistance carried out

This table resumes the fields of law where the assistance is requested per each topic in order to point out the legal issues frequently encountered by these projects. X-marks indicate where a specific topic has been particularly asked by the project or where the analysis of this topic has been really time-consuming.

	Data Protection	Consumer Protection	Liability	IPR	Taxation	Contract Law	Electronic Payments	IPL
AIMEDIA	X	X				X		X
TRADE	X	X	X			X		X
TRIP	X	X	X	X	X	X	X	X
COSMOS						X		X
INTERNET MEGASTORE	X	X				X	X	X
PETER				X				
FACTMERCHANT			X	X	X			X
CYBERBRAND	X							X
MEDICOM	X		X	X	X	X	X	X
NECTAR	X	X		X		X	X	
TELEPOLIS	X		X	X	X			

5. ISSUES OF THE ASSISTANCE

The process of assistance has underlined some specific key issues due either to the lack of responsiveness of the assisted projects, either to the very nature and limits of the ECLIP assistance. Those issues are the following :

5.1. Unawareness of the legal framework

The RTD projects we are currently assisting are largely unaware of the regulatory framework in which the project is developing. Most of the times they ask for a sort of 'legal package' to be integrated as such in the project. Therefore, there is a need to assess a way of collaborating with the project so as to consider the legal constraints along the design and development of their objectives.

This first task is made more difficult when the project to be assisted is not very clear. In such a case we have to create awareness on the legal constraints before starting the effective assistance.

In some cases, we fear that this awareness has not reached its goal. This might entail that the project is satisfied with our first and overall analysis of their legal constraints without feeling the need to implement and integrate, with a further assistance from ECLIP, an answer to these constraints in the design and development of their project.

5.2. Difficulty due to the time schedule of the project

Most of the projects to be assisted are in their middle or at the end. Therefore, to some extent , the legal analysis we carry out is sometimes not easy to integrate in the project. Legal constraints should be integrated and considered by e-commerce projects as soon as they start the development of their tools or services.

A similar difficulty could appear at the end of ECLIP if new projects request assistance at this moment. The assistance we could provide them should then be limited to the ECLIP's end and could not accompany the project until its own end.

Consequently, this highlights the need for a certain permanency of the ECLIP platform which should be able to accompany the electronic commerce initiatives or project from their beginning to their end.

5.3. Resources of the RTD projects for assistance

The assistance provided by ECLIP might be in some cases an additional burden for the projects, in terms of time, travels. In some cases, it is difficult to maintain a close and interactive collaboration between both projects when the assisted project has to comply with particular deadlines. This has sometimes lead to delays in the assistance foreseen.

Therefore, we would like to point out the need to contractualise the assistance so as to commit the projects. Another solution would be to plan the ECLIP intervention in the technical annex of the future assisted project. This point depends also on the permanency of the ECLIP tool.

5.4. Legal topics

It is self evident that amongst the fields of law covered by the ECLIP partners, some aspects are more demanded than others. It is the case namely for privacy, consumer protection, digital signature, electronic contract. Other topics are more hidden and their consideration does not appear immediately to the projects. Some topics are rarely relevant in the scope of assistance requested.

The table figuring under 4.12 provides an idea of the level of interest shown by projects for legal topics. This table highlights that the data protection, consumer protection, Intellectual property rights, contract law, and to a lesser extent taxation and international private law, are the most demanded topics. Liability and electronic payments appears to be less relevant for the projects. One reason thereof is perhaps that the assistance on liability of intermediaries and electronic payments imply that the project develop as such e-payments systems or integrates or plays the part of an intermediary.

ECLIP has had to develop a strategy to 'sell' the assistance on some topics. This implies that the consideration of such topics will mainly be done by the last projects we assisted.

It has also been necessary to reallocate in some cases the number of man-days from a legal topic to another. For instance, some man-days normally dedicated to liability issues have been used for privacy analysis since this topic has already consumed a great number of man-days.

5.5. Repetition of some fields of assistance

It should be noted that some demands for assistance might be very similar from a project to another. A consequence thereof is that the partner in charge of providing assistance can repeat and resume what has been elaborated in another framework while adapting it for the new project. Nevertheless, it entails that the topic of the assistance does not necessitate a new in-depth research. This can be considered as somewhat contrary to the objective of a university research and this can increase the risk of competition relating to other forms of legal consultancy services. Therefore, there is the need amongst the ECLIP partners to think about new ways of assistance, such as training or specific workshops, where the basic principles can be addressed with a number of assisted projects simultaneously.

6. Further assistance foreseen

The following projects : ECOS, COSEPPA, ELTRAMOS, SUPPLYPOINT and ECADEC have asked for ECLIP assistance.

Legal assistance in terms of creating awareness is equally provided to ESPRIT projects during our workshops and during EC- Cluster activities.

7. Conclusion

As a conclusion, we could state that generally the assistance works well and that the number of projects currently assisted or seeking for collaboration with ECLIP is increasing.

Besides, the ECLIP partners have managed to maintain a balance between the tasks, the re-partition of relevant fields and the type of projects. The number of man-days devoted to each projects, as planned in the technical annex , is constantly under review so as to allocate to new projects the number of man-days that were not consumed in others, or to allocate more man-days in the most relevant legal fields.

The procedure of assistance has been also reconsidered in order to face the need for an overall coordination of the assistance, whose CRID is finally responsible. Nevertheless, this task of assistance, previously not planned in the ECLIP workplan, has been largely time-consuming. Therefore, this task should be particularly considered in the future.

This coordination task has been completed by a necessary meeting between the ECLIP partners and the project seeking assistance so as to effectively be aware of the scope and needs of the project and to agree upon the field and scale of intervention of each ECLIP partner. Such meeting enables also ECLIP to create an overall awareness of the legal constraints and issues that might arise in the development of the project.

Finally, we should consider in the future the necessity to be more selective in the choice of the projects if their number keeps increasing. The projects whose needs and level of commitment are low should not be priorily assisted.

ANNEX 1 : Assistance to AIMEDIA on data protection and advertising regulations

Project Number:	**P26983**
Project Title:	**AIMEDIA**
Availability:	**R**

CEC Deliverable Number:	**P26983-D13-IGD-a1**
Contractual Date of Delivery to the CEC:	**September 30th, 1998**
Actual Date of Delivery to the CEC:	**October 14th, 1998**
Title of Deliverable:	**Customised secure advertising framework specifications**
Workpackage contributing to the Deliverable:	**WP 1**
Type of the Deliverable:	**S**
Authors:	**Mehrdad Jalali**

Abstract:

This Deliverable presents the specifications for the AIMedia customised secure advertising framework. First of all we show how intelligent agent technologies will be used to insure One-to-One marketing. The customised advertising approach is compared to current work on intelligent agent technology. The core technology behind One-to-One marketing is personal data, summarised in the user profile. We review the legal issues implied by the use and exchange of personal information, and conclude with constraints on the design of the framework. Technical solutions to secure data transfer over Internet as well as data protection are then presented, and are then integrated into the framework.

Keywords :

Targeted advertising, One-to-One marketing, security, intelligent agents, user profile, legislation

4. LEGAL CONTEXT

This part is the result of the collaboration between AIMedia and ECLIP, a European Esprit project, whose goal is to offer legal advice to other projects where this expertise is missing. ECLIP discusses the AIMedia requirements as stated in deliverable D11 and extended in this document, and confronts it to existing or emerging European directives and there national application.

Two aspects are dealt with : general advertising issues and personal data protection. Each section will outline the legal requirements that partners of the AIMedia project will have to comply with when providing some targeted advertising based on personal user profiles.

We conclude with design constraints the project must integrate as part of the customised secure advertising framework.

4.1 Advertising

The aim of the project is to develop a personalised and tailored-made advertising in order to promote purchases. According to the project, advertising should be considered as "helpful, exciting and enriching for the customer"[1], but one should keep in mind that advertising can be seen as intrusive.

As the targeted advertising the partners are developing represents a quite large number of communications, mainly individualised on the basis of the consumer's behaviour and purchases' habits, it is important that the consumer receives enough information enabling him to understand the meaning of the advertising and its consequences. Furthermore, it seems obvious that the consumer should be able to refuse such communications through an opposition mean: as this targeted advertising can be interpreted by the consumer as being intrusive, useless and annoying, the advertiser – namely the partners of the project – should prevent the consumer from leaving the site and never come back by offering him the possibility to refuse such advertising.

This section will first concentrate on providing general comments on advertising, i.e. to what extend the advertiser is bound by the content of the advertising, how an advertising can be differentiated from an offer, what consequences the type of medium used has on the advertiser.

Then the rights implied for consumers from this kind advertising will be described, namely any relevant information enabling the consumer to make up his mind on whether he can benefit from the advertising and decide either to accept it or refuse it – on the basis of an opposition right granted by the advertiser - if he believes that the advertising is useless and intrusive.

Finally, the legal rules applying at both European level and in Germany and the United Kingdom will be analysed, as well as any relevant extra-legal provisions.

---

[1] See deliverable P26983-D11-UCL-b1. "Generic requirements and first theoretical models" § 3.1.6 p.25.

4.1.1 Advertising: a brief outline

According to Directive 84/450/EC concerning misleading advertising[2], advertising is seen as "the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations"[3].

The obligations and duties described below fall on the advertiser, namely the person responsible for the advertising addressed to the consumer, and its content. In the project the advertiser should be heard as the partners themselves, namely Otto and Sainsbury.

4.1.1.1 Liability of the advertiser with regard to the content of the advertising

As regard the information contained in the advertising, the question raises as to know whether the advertiser is bound for the content of the advertising. This issue is of importance as it has the consequence that the advertiser would not be able to modify the terms described in the advertising when the consumer agrees with this content and decides to conclude the contract.

It can be considered, following what seems to be a dominating opinion in the doctrine[4], that the facts contained in the advertising bound the advertiser who cannot thus modify the content.

Otto Versand and Sainsbury shall therefore be aware of the fact that any information contained in their advertising is bounding: the terms and conditions cannot be modified once the consumer decides to conclude the contract.

4.1.1.2 Advertising vs. offer

Another important issue is related to the difference between advertising and offer: under what conditions an advertising can be considered as an offer? What consequences does the qualification of an advertising in offer has on the advertiser?

Legal effects of an advertising depend on its content: either the advertising identifies the essential parts of the contract, i.e. the object of the contract (product or service) and its price, or it does not clearly identify these essential parts.

If any offer to sell a product or supply a service is deemed as an advertising, any advertising is not deemed as an offer. To be considered as an offer, an advertising should clearly identify the object of the contract and the price[5]. In the first case above-described, the advertising should be considered as constituting an offer insofar as both the object and the price are mentioned. The legal consequence of this qualification is that the advertiser has to comply with the information contained in the advertising and to execute the contract according to the terms of the advertising.

---

[2] Directive of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, *O.J.E.C.* L. 250/17 of 19.09.1984

[3] Article 2 § 1.

[4] See " propositions pour une loi générale sur la protection des consommateurs ", rapport de la Commission d'Etudes pour la Refonte du Droit de la Consommation (CERDC), Belgian Ministry of Economic Affairs, 1995, pp. 82-83.

[5] See Cass. 9 mai 1980, *Pas.* I p. 1127 ; R.C.J.B. 1971 pp. 228-229.

Conversely, any advertising where both above-mentioned elements are not identified i.e. where the object of the contract is identified but not the price, would not be considered as an offer, enabling the advertiser to modify slightly the conditions[6].

4.1.1.3 Presentation of the advertising

1. – On-screen messages

The presentation of the communication chosen by the partners of the AIMedia project is mainly the inclusion of a personalised message directly on the screen, while the consumer is visiting the site. Indeed, partners of the project envisage to target existing consumers, meaning that "it is not until consumers have actually made the decision to visit the site that they will be exposed to the communications".[7]

In this hypothesis, no legal constraints in term of consumer consent are foreseen, as the consumer has taken, at his own initiative, the necessary steps to visit the site.

2. – Individual communications: e-mail messages

Another hypothesis would be to carry on contacts with the consumer through his e-mail address, as the consumer might, at a particular step of a transaction, introduce personal data including his e-mail address. The advertiser might be attracted to use this address for further individual communications. This possibility is however described in scenario 1 (short to medium term)[8], the project also describe as a mean to the development of 1 to 1 marketing e-mails: "once the consumer subscribes to a mailing-list with individual preferences, ha can receive tailored e-mails with specific information of offers"[9].

Such personalised communications fall under the scope of two European Directives: firstly the distance contracts Directive[10], secondly the Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data[11]: those two texts provide for a similar principle of *opt-out* in the frame of commercial communications. According to article 14 (b) of the privacy Directive, the data subject shall be provided with the right to "object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing (...)". Article 10 § 2 of the distance contracts Directive lays down the opt-out principle: "means of distance communication which allow individual communications may be used only where there is no clear objection from the consumer".

---

6 Such modifications relate anyway on elements that are not clearly defined in the advertising: any further information will have the consequence to make the advertising becomes an offer, bounding the advertiser by its content.

7 See deliverable p.7.

8 See deliverable p.22.

9 See deliverable p.25.

10 Directive 97/7/EC of 20 May 1997 concerning the protection of consumers with respect to distance contracts O.J.E.C. L.144/19 of 4.06.1997.

11 Directive 95/46/EC of 24 October 1995 *O.J.E.C.* L.281/31 of 23.11.1995.

Unlike the opt-in technique[12], the advertiser has no need to require the prior consent of the consumer to receive the advertising, but he should be aware of the possible objection to receive individual communications.

Consequently, the advertiser shall take the necessary arrangements to be informed of a possible opposition of the consumer to receive such individual communications. The privacy Directive goes further by stating that the data subject (in this case the consumer) shall be "informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses". The Directive imposes upon the Member States the obligation to take the necessary measures to ensure that data subjects are aware of the existence of this right but it does not mention on who this obligation should be imposed.

If individual messages are foreseen to be sent through e-mail by Otto Versand and Sainsbury, the following obligations will have to be complied with:

take the necessary arrangements to know if the consumer has clearly objected to receive individual communications,

inform consumers about their right to object, free of charge, to receive such individual communications[13].

4.1.2 Information of the consumer

When broadcasting their advertisements, Otto Versand and Sainsbury have a double duty of information: they shall first inform their consumers about the advertising itself: what is the aim? What consequences does it have for them? etc. Then, they shall offer them the possibility to object to this kind of advertising with, here again, an information on the consequences of the objection.

Such obligations of information are not stated in any text at the European level, but it does correspond to concrete expectations of consumers: if the screen is overwhelmed by commercial communications, consumers might feel frustrated if no prior explanations has been forwarded to them about those communications, the risk being that they decide to stop the connection with the site. A similar explanation applies to the possibility to object: consumers feel better understood if they are given a rational choice to make, up to their own wills and expectations.

4.1.2.1 Time and content of the information

1. – When does the consumer shall be informed?

Targeted consumers are, according to the statements of the project, existing consumers, meaning consumers having already entered the site and who know already the site. It is without doubt that these consumers will see a major change on the site, as such targeted

---

[12] Article 10 § 1 of the distance contracts Directive foresees the opt-in technique: "the use by the supplier of the following means [of distance communication] requires the prior consent of the consumer: automated calling systems without human intervention (automatic calling machine), and facsimile machines (fax)".

[13] The information on the right to object could be mentioned within the first e-mail message.

advertising did not exist at the time of their previous visits. Therefore, as soon as the consumer enters the site and is "in the shop", he shall receive information about the targeted advertising.

2. – How the consumer shall be informed?

Concretely, the site should mention on its first page the existence of the targeted advertising and should incite consumers to call for further information. An icon could be appropriate but should be made attractive enough in order to incite consumers to click on it. However, a minimum information should, at least, be placed on the screen.

A difficulty might appear if the consumer does not go for information: unless the site blocks further access if the information has not been consulted - which is rather uncertain - it cannot oblige the consultation. The site should thus leaves the possibility to come back to the information later during the visit[14] and at any time of the visit.

Likewise, the site should offer a distinction between consumers having already consulted the information, and those who have not. This would avoid to oblige a consumer to consult each time the information.

3. – What information shall the consumer receive?

A rational and comprehensive information shall be forwarded to the consumer. It is of crucial importance that he understands the goal of the advertising and how he can benefit from it.

Having these points in mind, it is considered that the following information should be granted to the consumer[15]:

- what is the aim of the advertising (i.e. it should be stated clearly that the aim is to increase purchases, not only to inform consumer on other products),
- how the advertising is made personal,
- how the advertising is presented,
- what practical consequences does it have as far as the connection is concerned: does it increase the length of connection, does it imply additional costs charged to the consumer, etc.
- how frequent advertising appears on the screen,
- how the consumer can take advantage of the advertising, etc.

Actually, the information forwarded to the consumer shall make him able to decide whether he agrees to receive it or not: any relevant information to help him make up his mind should be granted.

Finally, the consumer should receive the information about the possibility to object to this kind of advertising.

---

[14] A consumer who is in a hurry might decide not to consult the information, and be later surprised by the communications appearing on the screen during the visit of the site. It is therefore useful for him that this information is easily accessible at any time.

[15] This list is indicative and can be subjected to modifications.

4.1.2.2 Right to object

The possibility to refuse receiving targeted advertising should be given to the consumer without giving any reason and without charges.

1. – Form of the objection

The objection could be materialised in a form to fill or a icon to click on. However, it is recommended not to limit the opposition to a simple click, in order to avoid any misuse and involuntary objections.

Whether the choice is made between a form to fill, an icon to click or any other possibility, it would be relevant to impose a confirmation of the choice.

2. – Time of objection

Like the information on the advertising, it is necessary that the consumer be offered the possibility to object at different time of the visit. The objection could be given:

at the time the information on the advertising is given, or

later during the visit, or

at the occasion of a next visit.

An icon or something similar could be used and should be visible from any step of the visit to allow the consumer to object at any time.

The site could also envisage the possibility for the consumer to come back on the objection and to decide to agree on receiving targeted advertising.

3. – Consequences of the objection

In the "objection form" or in the "objection icon", information should be given on the consequences the objection means for the consumer, especially if Otto Versand and Sainsbury foresee a different treatment between consumers agreeing on receiving the advertising and others.

Likewise, if a possibility to come back on the objection during a next visit is foreseen, consumers should be informed of such possibility and how to manage it.

4.1.3 Legal and extra-legal rules regulating advertising

4.1.3.1 At the European level

1. – The misleading and comparative advertising Directive

An advertising Directive was first adopted in 1984 concerning exclusively misleading advertising[16]. This Directive had to be implemented by the Member States by 1 October 1986 at the latest. Then the European Commission expressed the wish to go further in the protection of consumers in the field of comparative advertising, by allowing it under strict conditions.

[16] See note 2.

This new Directive[17] adopted on 16 October 1997, is intended to amend Directive 84/450. This Directive has to be implemented by Member States at the latest 30 months after its publication in the Official Journal of the European Communities, so by the 23 April 2000.

1.1. – Misleading advertising[18]

Misleading advertising is defined as "any advertising which in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect their economic behaviour or which, for those reasons, injures or is likely to injure a competitor"[19].

In determining whether an advertising is misleading, account should be taken of all its features, and in particular of any information it contains concerning:

the characteristics of goods or services, such as their availability, nature, execution, composition, method and date of manufacture or provision, fitness for purpose, uses, quantity, specification, geographical or commercial origin or the results to be expected from their use, or the results and material features of tests or checks carried out on the goods or services;

the price or the manner in which the price is calculated, and the conditions on which the goods are supplied or the services provided;

the nature, attributes and rights of the advertiser, such as his identity and assets, his qualifications and ownership of industrial, commercial or intellectual property rights or his awards and distinctions.

In the frame of an administrative or judicial control of those provisions, the Directive mentions that the advertiser may be requested to provide evidence as to the accuracy of factual claims in advertising if, taking into account the legitimate interests of the advertiser and any other party to the proceedings, such a requirement appears appropriate on the basis of the circumstances of the particular case. If such evidence is not furnished by the advertiser or deemed insufficient by the court of the administrative authority, the factual claims will be considered inaccurate, opening either a cessation procedure or a prohibition of publication[20].

1.2. – Comparative advertising

The purpose of the Directive is "to protect consumers, persons carrying on a trade or business or practising a craft or profession and the interests of the public in general against misleading advertising and the unfair consequences thereof and to lay down the conditions under which comparative advertising is permitted"[21].

---

17 Directive 97/55/EC of the European Parliament and the Council of 6 October 1997 concerning misleading advertising so as to include comparative advertising. available on the Internet: http://www.europa.eu.int/comm/dg24/policy/developments/comp_adve/comp_adve02_en.html

18 http://www.europa.eu.int/comm/dg24/policy/developments/misl_adve/misl_adve01_en.html

19 Article 2 § 2 of Directive 84/450.

20 Depending on whether the advertising is already published or it has not been published but its publication is imminent. See article 4 § 2.

21 Article 1 (2) of Directive 97/55.

Comparative advertising is heard as "any advertising which explicitly or by implication identifies a competitor or goods or services offered by a competitor"[22].

The conditions for allowing comparative advertising are rather strict as they are, on the one hand, devoted to grant a better information to consumers, but on the other hand the wish is to avoid any distortion in competition through any detriment to competitors and adverse effect on consumers' choice. Therefore, the following conditions have to be fulfilled:

- the advertising shall not be misleading;
- the advertising shall compare goods and services meeting the same needs or intended for the same purpose;
- the advertising shall compare objectively one or more material, relevant, verifiable and representatives features of those goods and services, which may include price;
- the advertising shall not create confusion in the market place between the advertiser and a competitor or between the advertiser's trade marks, trade names, other distinguishing marks, goods or services and those of a competitor;
- the advertising shall not discredit or denigrate the trade marks, trade names, other distinguishing marks, goods, services, activities, or circumstances of a competitor;
- for products with designation of origin, the advertising shall relate in each case to products with the same designation;
- the advertising shall not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products;
- the advertising shall not present goods or services as imitations or replicas of goods or services bearing a protected trade mark or trade name.

All these provisions are of strict application, i.e. Member States are not allowed in the implementation process to adopt stricter rules that could possibly lead to the prohibition of comparative advertising. It is therefore highly recommended that advertisers already base their practice on those principles if they wish to provide some comparative advertising.

2. – Green Paper on commercial communications [23]

The advent of the Information Society led the European Commission to formulate four general remarks as far as the commercial communications are concerned:

- digital communication infrastructures offer a new medium of communication for commercial messages; a large growth of marketing activities on the network is expected;
- broadcasting speed will ease cross-border commercial communications;
- distance sales will speed up due to the interactive possibilities of the network;

---

22 Article 1 (3).

23 COM (96) 192 final.

- network operators will offer new communication services at lower prices.

4.1.3.2 At the English and German levels

1. – The United Kingdom

Advertising is in part controlled by legislation in the interests of consumer protection, but there is in addition a comprehensive Code of Practice promoted by the independent Advertising Standards Authority.

1.1. - Legislation

Like all other European countries, England has no specific legislation addressed to advertising on the Internet.

The misleading Directive has been implemented in England in 1988 in a law on 'the control of misleading advertisements regulations'[24]. Advertising is defined in a similar war than the Directive, as well as the misleading character of the advertising, namely an advertising that in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and that, by reason of its deceptive nature, is likely to affect their economic behaviour or, for those reasons, injures or is likely to injure a competitor or the person whose interests the advertisement seeks to promote[25].

Any complaint regarding a misleading advertisement should be brought to the Director General Fair Trading. the law then describes the procedure to be followed as to the complaint, which does not directly concern AIMedia partners. All is important is the definition of the misleading character of an advertising that is the same in the European Directive.

Comparative advertising is allowed by the Trade Marks Act of 1994 unless it is detrimental to or unfair to a competitor. Section 10 (6) allows the use of a trade mark for the purpose of identifying goods and services as those of the owner but prohibits such use when:

- it is not in accordance with honest practices in industrial or commercial matters, or

- it takes unfair advantage of or is detrimental to the distinctive character or reputation of the competitor.

1.2. – The British Codes of Advertising and Sales Promotion[26]

The ninth edition of the Advertising Code and sixth edition of the Sales Promotion Code came into force on 1st February 1995. The Codes apply to sales and advertisement promotions, irrespective of the way they are broadcast. Although slight differences are foreseen in the Advertising Code and the Sale Promotion Codes, similar principles apply to advertisements and sales promotions. The Codes are divided as follows:

- CAP (Committee of Advertising Practice) members,

---

[24] Law n° 915 of 23 May 1988.

[25] See paragraph 2 (1) and (2).

[26] Available on the Internet at the following address: http://www.asa.org.uk

- Introduction,
- Advertising Code,
- Sales Promotion Code,
- Specific Rules,
- Cigarette Code,
- Legislation,
- How the system works,
- Index.

As any auto-regulatory rules, the Codes have no legal status but they however represent an important source of reference for advertisers.

1.2.1. – General provisions

The following principles are set up in the Code[27]:

- *General principles*

Advertising should be legal, decent, honest and truthful, framed with a sense of responsibility to the consumer and conforming to the principles of fair competition. It should contain nothing that is likely to cause serious widespread offence. Particular care should be taken to avoid causing offence on the grounds of race, religion, sex, sexual orientation or disability. Obvious untruth or exaggerations that are unlikely to mislead and incidental minor errors and unorthodox spellings are all allowed provided they do not affect the accuracy or perception of the advertisement in any material way.

No advertisement should mislead by inaccuracy, ambiguity, exaggeration, omission or otherwise. Advertisers should not exploit the credulity, lack of knowledge or inexperience of consumers, they should not use shocking claims or images merely to attract attention or to cause fear or distress. However, advertisers may use an appeal to fear to encourage prudent behaviour or to discourage dangerous or ill-advised actions.

- *Liability*

Advertisers have the primary responsibility for ensuring that their advertisements are legal. Advertisements should contain nothing that breaks the law or incites anyone to break it, and should omit nothing that the laws requires.

- *Price*

Advertisers should ensure that prices mentioned in the advertising are clear and relate to the product advertised and should ensure that prices match the products illustrated. If the price of a product is dependent on the purchase of another, the extent of any commitment by consumers

[27] The principles described are those set up in the Advertising Code, but they should be heard as applying also to Sales Promotions.

should be made clear. Price claims such as 'up to' and 'from' should not exaggerate the availability of benefits to be obtained by consumers.

- *Free offers*

There is no objection to making a free offer conditional on the purchase of other items. Consumers' liability for any costs should be made clear in all material featuring the offer. An offer should only be described as free if consumers pay no more than:

a. the current public rates of postage

b. the actual cost of freight or delivery

c. the cost, including incidental expenses, of any travel involved if consumers collect the offer.

Advertisers should make no additional charges for packing and handling.

Advertisers must not attempt to recover their costs by reducing the quality or composition or by inflating the price of any product that must be purchased as a pre-condition of obtaining another product free.

- *Availability of products*

Advertisers must make it clear if stocks are limited. Products must not be advertised unless advertisers can demonstrate that they have reasonable grounds for believing that they can satisfy demand. If a product becomes unavailable, advertisers will be required to show evidence of stock monitoring, communications with outlets and the swift withdrawal of advertisements whenever possible. Products which cannot be supplied should not normally be advertised as a way of assessing potential demand.

Advertisers must not use the technique of switch selling, where their sales staff criticise the advertised product or suggest that it is not available and recommend the purchase of a more expensive alternative. They should not place obstacles in the way of purchasing the product or delivering it promptly.

- *Guarantees*

The full terms of any guarantee should be available for consumers to inspect before they are committed to purchase. Any substantial limitations should be spelled out in the advertisement.

- *Comparisons*

Comparisons should be explicit or implied and can relate to advertisers' own products or to those of their competitors; they are permitted in the interests of vigorous competition and public information. Comparisons should be clear and fair. The elements of any comparison should not be selected in a way that gives the advertisers an artificial advantage. Advertisers should not unfairly attack or discredit other businesses or their products. The only acceptable use of another business's broken or defaced products in advertisements is in the illustration of comparative tests, and the source, nature and results of these should be clear.

- *Exploitation of goodwill and imitation*

Advertisers should not make unfair use of the goodwill attached to the trade mark, name, brand, or the advertising campaign of any other business. No advertisement should so closely resemble any other that it misleads or causes confusion.

- *Identifying advertisers and recognising advertisements*

The identity and status of the advertiser should be clear: if their address or other contact details are not generally available they should be included in the advertisement. Advertisers, publishers and owners of other media should ensure that advertisements are designed and presented in such a way that they can be easily distinguished from editorial.

1.2.2. – Specific provisions

Besides the general provisions, the Codes contain provisions aimed at protecting either specific categories of consumers, or specific categories of products.

- *Protection of children*

The will to protect children is clear within the Codes: any advertisement or promotion addressed to or featuring children should not contain anything likely to result in their physical, mental or moral harm. They should not exploit their credulity, loyalty, vulnerability or lack of experience.

- *Environmental claims*

The use of claims such as 'environmental friendly' or 'wholly biodegradable' should not be used unless the advertiser ca, provide convincing evidence that their product will cause no environmental damage.

- *Health and beauty products and therapies*

Specific provisions are foreseen on medicinal products, vitamins, minerals and food supplements, cosmetics, hair and scalp and slimming. Those provisions contain detailed regulations aimed at forbidding advertisers to discourage people from having essential treatment: medical advice is needed for serious or prolonged ailments and advertisers should not offer medicines or therapies for them[28].

- *Alcoholic drinks*

The drink industry and the advertiser should accept a responsibility for ensuring that advertisements contain nothing that is likely to lead people to adopt styles of drinking that are unwise; their messages should not encourage excessive drinking.

- *Cigarette Code*

No advertisement should incite people to start smoking, it should not encourage smokers to increase their consumption or smoke to excess, smokers should not be encouraged to buy or stock large quantities of cigarettes[29].

---

[28] For a more detailed analysis of the provisions, see points 50.1 to 51.12 of the Codes.

[29] See points 66.1 to 66.26

2. – Germany

2.1. – Misleading advertising

Advertising is not regulated per se in Germany, provisions on misleading advertising are found in the Unfair Competition Act of 7 June 1909 (Gesetz gegen den unlauteren Wettbewerb - UWG): according to article 3, anyone who makes misleading statements in the course of a business activity for competition purposes, especially on the quality, the origin, the way of production, the calculation of prices of goods or services, prices lists, the way of supply or the source of supply of goods, on awards on the cause of the selling or on the amount of stocks is liable for damages and injunction[30].

Misleading advertising is therefore prohibited on the basis of unfair competition. This prohibition is strengthened by the German courts.

2.2. – Comparative advertising

Article 1 of the Unfair Competition Act states that anyone who carries out acts in the course of business competition purposes and infringes good morals is liable for injunction and damages. Traditionally, this provision was interpreted by the courts as prohibiting comparative advertising.

Recently, the Federal Court of Justice changed this interpretation as to implement the European Directive 97/55/EC on comparative advertising. The Court now considers comparative advertising allowed insofar as conditions set up in the Directive are complied with[31].

2.3. – Specific rules

Advertising of tobacco is prohibited under a Foodstuff and articles of daily use Act[32]: article 22 prohibits the advertisement of tobacco products as well as advertisements evoking the impression that the use of tobacco products is not causing health problems or that might influence teenagers to smoke.

The Act on the distribution of writing and media contents which may be morally harmful to youth[33] contains a prohibition of harmful advertisements accessible to young people.

4.2 Privacy issues

4.2.1 Introduction

The European Union directive on the protection of individuals with regard to the processing of personal data[34] must be transposed into the legislation of the Member

---

30 Non official translation.

31 Federal Court of Justice, NJW 1998, pp.2208-2212, judgement of 5 February 1998.

32 Lebensmittel und Bedarfsgegenständegesetz – LMBG.

33 Gesetz über die Verbretung jugendgefährdender Schriften und Medeininhalte – GjSM.

States by October the 24th of this year, and will from this date become a legally binding instrument. While the directive may require some modifications in the European countries' law, most of these countries already embody the principles of the directive. An overview of the regulatory framework in action in the context of electronic commerce in the United Kingdom and in Germany cannot therefore avoid the analysis of this directive[35]. Furthermore in Germany, article 2 of the Federal Act Establishing the General Conditions for Information and Communication Services[36] entitled "Act on the Protection of Personal Data Used in Teleservices"[37] will apply, according to §2 of the Information and Communication Services Act to "all electronic information and communication services which are designed for the individual use of combinable data such as characters, images or sounds and are based on transmission by means of telecommunications (teleservices)" and in particular to goods and services offered and listed in electronically accessible data bases with interactive access and the possibility of direct order.

The aim of this section is to outline the main obligations arising from these legal instruments which must be respected in AIMedia projects such as Otto Versand and Sainsbury.

4.2.2 Scope and Identification

4.2.2.1 Personal data

The directive applies to the processing of personal data wholly or partly by automatic means[38]. One of the first questions which arise therefore is to determine whether or not personal data is being processed in the context of the electronic commerce activities developed by Otto Versand or Sainsbury.

The Directive adopts a very broad definition of the term "personal data" so as to include any information relating to an identified or identifiable person ("data subject"). The person may be "directly" identified (by reference to his name, for example) or can be "indirectly" identified by reference to specific characteristics of that person, in particular by reference to an "identification number", or to one or more factors specific to his "physical, psychological, mental, economic, cultural or social identity". It must be underlined that the directive does not therefore apply to data regarding legal persons.

Two types of data can be identified in AIMedia scenarios : Collected data is data collected directly from the data subject either during registration to the service or when

---

[34] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995, p.31 (hereinafter general directive).

[35] We will leave out the specific issue of the transfer of personal data outside the European Union seeing as these types of transfers are not envisaged in the AIMedia projects.

[36] Informations-und Kommunikationsdienste-Gestz – IuKDG of August 1 1997 (hereinafter Information and Communication Services Act) ;

[37] Teleservices Data Protection Act – Teledienstedatenschutzgestetz (hereinafter TDDSG)

[38] See article 3.1 of the directive.

filling in a form during the data subject's visit to the site. Extracted data covers data deduced from automatic data mining. For example how can either of the categories of goods purchased, articles ordered, pages visited, catalogue consulted and customer data be correlated to provide additional information than that initially collected from the data subject himself?

4.2.2.1.1 Collected Data

A distinction must be made here between existing customers entering the site and new prospective customers. In the context of existing customers who enter a customer or card number when entering the website, there is no doubt that personal data about that customer is being processed since this number is linked to identification of the customer (when taking out a card Sainsbury customers are asked to give some basic personal data such as the size of their household, address, age,...). As for new customers they could be asked upon entering into the site to fill in a form requesting personal data. However if no personal data is introduced by the data subject himself will the directive still apply?

Users inevitably leave an electronic trace when entering the Net. This trace takes the form of an IP address (Internet protocol address), i.e. a series of numbers. Whether or not the IP address relates to an "identifiable" person is not straightforward.

A distinction must be made between a dynamic IP address and a fixed IP address :

A dynamic address is a numeric routing number that is allocated by the Internet Access Provider (IAP) to a computer for a specific session on the Internet. The access provider is the one who can link the IP address to an identified person or computer. Very often, however, the user is asked by the host to give his name or e-mail address. The host can then "put a name" on the IP address and follow the person during all his operations. Unless the user reveals further information or there exists a link between the host site and the IAP, the sites that are being visited can only associate the IP address with the IAP but not with the user of the Internet.

In contrast a fixed IP address will always identify the same specific computer for every session on the Internet. However once the computer has been identified, does this mean that we are in the presence of personal data which relates to an "identified" or "identifiable" individual ?

To determine whether a person is "identifiable", account should be taken of all the means likely reasonably to be used by the controller, or by any other person, to identify the said person[39]. Indirectly identifiable information is therefore limited to information which can be reasonably linked to an identified person. Does an IP address which reveals the identity of the computer used identify the user behind the computer ? A fixed IP address is more likely to be qualified as personal in the same way as licence plate numbers or telephone numbers have been qualified as personal data by the national data protection authorities. This is even more true in the context of the services offered by Sainsbury and Otto Versand which rely on the identification of the person so as to establish a personalised service.

[39] § 26 of Directives' recitals

4.2.2.1.2 *Extracted data*

Extracted data covers any data which is not directly submitted by the data subject himself but is deduced from consumer behaviour for example. To the extent that this information can be linked to an identified or identifiable individual, it must be considered as personal data in the eyes of the directive[40].

4.2.2.2 Controller

The directive provides for a number of duties and obligations incumbent on the " controller ". One must therefore determine whether Otto Versand or Sainsbury can be qualified as controllers.

Identification of the "controller" is one of the primary problems one is faced with when applying the directive to electronic commerce transactions characterised by their numerous actors. Amongst others, one can identify: Internet access providers, Internet software editors, vendors, marketing companies, and banks and financial institutions offering means of payment. According to article 2.d of the directive, the controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

In the processing of data so as to establish personal profiles, a distinction must be made between the simple shopping site service by Otto Versand or Sainsbury and the more complex scenario of a consortium of non competing companies in which personal profiles are established by the sharing of data amongst actors[41].

In the first scenario Otto Versand and Sainsbury establish their own personal profiles from data collected by the use of their services and by questionnaires filled in by customers visiting their sites. Each company determines the purpose of the service offered and the means by which this service is carried out and must therefore undoubtedly each be qualified as a controller in the terms of the directive. If the retailers share any information amongst themselves so as to establish complete customer profiles, they remain the controllers of the processing and the communication of the data must respect the principles laid down in the directive (see below).

In the context of a consortium of companies, gathering information from the different retailers in a shopping mall so as to establish consumer profiles and dispatching the information to the retailers, the consortium in itself, as a separate legal entity, could be qualified as the controller since it determines the means and purposes of the processing.

---

[40] The person is not necessarily identifiable : an identity cannot always be deduced from consumer habits. Purchases may not necessarily correspond to a person's needs or profile. A buyer could be buying for someone else. for example.

[41] This scenario corresponds to the "personal shoppers " scenario (see 3.2.3.2. of P26983-D11-UCL-b1) where the shopper is offered a personal agent who acts on the shoppers behalf. Information from any of the shopping activities may be shared on a common profiling basis between the retailers with the customer's consent.

4.2.3 Principles to be respected

The directive lays down a series of principles which must be respected by the controller. We will examine each one of these principles underlying the main implications for the AIMedia project.

4.2.3.1 The Purpose Limitation Principle

4.2.3.1.1 Personal data must be processed fairly and lawfully (article 6) .

"Fair" processing implies a maximum of openness. An individual's personal data cannot be processed for any hidden or occult reasons. Personal data may only be collected in a transparent way (this principle is guaranteed by the right of information, granted to the data subject in articles 10 and 11).

"Lawful" processing implies the respect of the national provisions taken in compliance with Chapter II of the directive.

4.2.3.1.2 Personal data must be processed for specified, explicit and legitimate purposes

Personal data may only be processed for specified and explicit purposes. This obligation compels the controller to determine at the outcome the exact purpose for which he intends to process personal data[42]. The determination of the purpose by the data controller must be sufficiently precise to enable the data subject to control every use of his personal data. For example, the purpose behind the OTTO project is not only the sale of goods electronically, but also and more importantly, the processing of personal data so as to establish personal profiles in view of offering a specially customer-tailored range of services, articles and promotions and thus improve seller-consumer-relationships.

The purposes for which personal data are processed must be legitimate and must be determined at the time of collection of the data (article 6.1.b). The very aim of data protection - the respect of the fundamental rights and freedoms of natural persons - implies that the purpose of the processing cannot rightly violate these rights and freedoms without a legitimate cause. The purpose must therefore be necessary in the eyes of a company or of the community in general. One must therefore balance the right of the individual to see his right to privacy preserved with the public or private interest to process the data. The final evaluation of the legitimacy of the purposes depends on the appreciation of the courts or of specialised data protection authorities.

3) Personal data may not be further processed in a way incompatible with the purposes for which the data was collected

The fact that personal data may not be processed in a way "incompatible " with the purposes for which the data was initially collected, does not exclude the use of the data for secondary purposes, but does limit the extension of the use of the data. Since the

[42] This obligation is further reflected in the data subject's right to be informed. See below.

directive aims at ensuring a maximum of openness with regard to the data subject, any intended non obvious purpose in relation with the purpose for which the data was initially collected could be regarded as "incompatible". The idea is not to avoid the use of the data for other purposes, but rather to avoid that under the cover of the initial purpose for which the data was collected, the data is reused for other purposes thereby circumventing the protection afforded by the principles stipulated in the directive. The uses considered as "incompatible" must be viewed as a new processing triggering the respect of the duties and obligations incumbent on the controller (see below).

As regards the services selling goods on Internet, customers will assume that the personal data that they may be requested to give when accessing the data base, will be used only in order to deliver the goods and bill their purchase. The establishment of personal profiles of the clients to target the clientele will not necessarily be considered as an obvious use of his data by the data subject unless the controller has informed the data subject prior to his use of the Internet. Similarly the communication of personal data to third parties does not come under the initial purpose for which the data was collected and may not necessarily be considered as compatible. In such a case the transmission in itself can be viewed as a new purpose in itself, respectful of the data protection principles enacted in the directive[43].

4.2.3.2 Grounds for processing of personal data

Article 7 of the Directive lays down the grounds justifying the processing of personal data. These grounds correspond to the circumstances considered by the European Community as allowing the processing of personal data. In order to be lawful, the processing of data must rely on one of these grounds, in addition to the fact that it must respect the obligations deriving from the legitimate purpose principle. Similarly in Germany the Teleservices Data Protection Act (TDDSG) provides that "personal data may be collected, processed and used by providers for performing teleservices only if permitted by this Act or some other regulation or if the user has given his consent"[44]. We will therefore also examine the purposes retained by the German TDDSG permitting the processing of personal data.

4.2.3.2.1 Article 7 of Directive

In the context of electronic commerce transactions, three justifications laid down in article 7 can more precisely be retained :

i) "The data subject has unambiguously given his consent" (article 7.a) :

Express written consent is not required. Any customer introducing his own personal data in order to purchase a good, could be considered as consenting to the processing of his personal data for this specified purpose. The introduction of further data in order to

[43] The purpose must be legitimate and explicit, the data subject will need to be informed. For the communication of sensitive data, the data subject could be required to give his explicit consent.

[44] §3 of TDDSG

obtain a personalised service could also be equated to the data subject giving his consent.

The data subject's consent must in any event be freely given[45] : there should be no pressure on the individual to obtain this consent. Free consent also implies that when a user is presented with a screen demanding personal data for further access, the fact that he refuses to go further should not be recorded or held against him.

The consent must also be informed, which means that vendors should inform each potential user of the service unequivocally about what he intends to do with the data and the risks this could incur for his privacy (see below, right to be informed). This enables the data subject to balance these risks against the expected benefits.

Lastly, the consent must be specific, it must relate to particular uses of the data for specified purposes. Any modification of the purpose which is incompatible with the initial purpose, requires a new consent. For example, if the data subject introduces personal data in the context of goods offered by OTTO, he does not necessarily consent to the transmission of his data to Sainsbury.

The interactivity characterising networks offers a special interest as regards the consent. Instead of a consent given once and for all at the start of a series of operations, interactivity enables you to modulate your consent. A message can appear on the screen at different times announcing "if you want to go further, you must consent to give such or such information". You can accept part of the operations but refuse to give more data at a certain point of the processing, or for a certain part of the service offered. Moreover, you can accept certain reuses announced but not all : you can tick off the cases corresponding to the accepted or refused uses of your personal data. Opting-in or -out methods acquire an immediate and effective dimension through interactivity.

ii) "Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (article 7.b).

A user may be requested to introduce certain personal data in order to obtain certain goods (his name and address so that the goods can be forwarded to him, his credit card number so that the goods can be billed,...). Only the data "necessary" for the performance of the contract may be processed. Therefore when one can do without personal data for the performance of a contract, one should not require it.

iii) "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where

[45] The data subject's consent is defined in article 2.h. of the Directive as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

such interests are overridden by the interests or fundamental rights and freedoms of the data subject..." (article 7.f).

This provision justifies the processing of personal data where it is in the legitimate interest of a natural or legal person, provided that the interests of the data subject are not overriding. This means that if the interest of a person in receiving personal data prevails over the data subject's interest not having his data communicated, data may be transferred. This is also true even when the data subject's interest in retaining his data is equivalent to the third party interest. It is only when the data subject's interest prevails, that the data relating to him may not be processed or communicated.

4.2.3.2.2 Principles for the processing of personal data under the TDDSG

According to the TDDSG, personal data may be collected, processed and used by providers for performing of teleservices only if permitted by the Act itself or some other regulation or if the user has given his consent. Similarly, the provider may use the data collected for the performing of teleservices for other purposes only if permitted by the Act itself or by some other regulation or if the user has given his consent.

i) Anonymity and User profiles

The provider must offer the user anonymous use and payment of teleservices or use and payment under a pseudonym to the extent technically feasible and reasonable[46]. Personal data relating to the use of several teleservices by one user are to be processed separately and a combination of such data is not permitted unless it is necessary for accounting purposes. Furthermore user profiles are permissible under the condition that pseudonyms are used. Profiles retrievable under pseudonyms shall not be combined with data relating to the bearer of the pseudonym[47].

The German legislation therefore imposes stringent limits to the sharing of information between teleservices such as OTTO and Sainsbury and to the establishment of user profiles without the consent of the data subject.

ii) Contractual data

According to the TDDSG §5, the provider may collect, process, and use personal data of a user to the extent necessary the data are required for concluding with him a contract on the use of teleservices and for determining or modifying the terms of such a contract (contractual data).

iii) Utilisation and accounting data

The provider may collect, process, and use personal data of a user concerning the use of teleservices only to the extent necessary to enable the user to utilise teleservices (utilisation data) or to charge the user for the use of the teleservices (accounting data)[48]. The TDDSG further provides that utilisation or accounting data shall not be transmitted to other providers

[46] §4 (1) of TDDSG

[47] §4 (2) and (4) of TDDSG

[48] §6(1) of TDDSG

or third parties. The only data that a provider offering access to the use of teleservices can transmit to other providers whose teleservices have been used by the user, are anonymised utilisation data for the purposes of their market research and accounting data to the extent necessary for collecting a claim. This provision seems to imply that if Otto Versand and Sainsbury, for example, intend to share information regarding the use of their services so as to obtain the most complete personal profile of their customer as possible, they will only be permitted to do so if the data subject has given his consent to this transfer.

iv) Data subject's consent

If the provider intends to use personal data for other purposes than those mentioned above, he must find grounds in another regulation or obtain the data subject's consent.

According to §3(6) of the TDDSG, before giving his consent the user must be informed of his right to withdraw his consent at any time with effect for the future. The consent can be declared electronically if the provider ensures that: such consent can be given only through an unambiguous and deliberate act by the user, consent cannot be modified without detection, the creator can be identified, the consent is recorded and the text of the consent can be obtained by the user on request at any time.

As concerns the processing and use of contractual data (data required for the concluding of a contract on the use of teleservices) for the purpose of advertising, market research or for the demand-oriented design of teleservices, §5 (2) provides that the consent must be explicitly given.

4.2.3.3 The Prohibition of Processing of Sensitive Data (article 8)

Subject to a number of exceptions set out in article 8.2, the processing of certain categories of data is prohibited according to article 8.1 of the Directive. This prohibition covers any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Any messages or data bases containing such data, will therefore need to find grounds within article 8.2. in order to be processed.

To the extent that profile information reveals an individual's morals as illustrated by an individual's consumer habits, such profiling comes within the ban of article 8.1. Similarly the electronic commerce activities linked to goods that reveal sensitive information fall within the scope of article.

The data subject's explicit and informed consent is probably the safest course to follow when one decides to process sensitive data relating to an individual (article 8.2.a). The other most obviously eligible ground to process sensitive data is when such data have been manifestly made public by the data subject[49] (in answering a questionnaire he has marked his preference for gay activities, or his religion, for example).

[49] Article 8.2.e of the directive

4.2.3.4 Data Quality

Both the directive and the Teleservices data protection act require a level of quality for the personal data that is being processed. The controller must ensure the respect of these principles.

1) Personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed.

The criteria of data adequacy are designed solely to ensure a necessary and sufficient link between the information and the purpose of the processing. For each finality, one must question whether or not there is a sufficient connection between the purpose and the data collected. Any irrelevant data must be discarded.

In the context of AIMedia projects, the data collected must therefore always ensure a sufficient link with the purpose of offering a specially customer-tailored range of products, services and promotions. If the collection and use of data such as the customer's name, address, number of persons in their household, hobbies and preferences can be justified as offering a sufficient link with the service offered, this could not be said of data such as the person's passport number or place of birth.

It must be pointed out that the targeted marketing offered requires more information to be given prior to the offering of the service, than the traditional distance selling of goods. Indeed in order be able to offer the most personalised service possible, the vendor will require a number of data before the goods are actually proposed, so as to offer goods corresponding to the person's needs (age, hobbies, sex, ...). The criteria of data adequacy could therefore enable the processing of more data than in a traditional environment.

The TDDSG also restricts the data which may be processed in the framework of teleservices. According to §3 (4) of the Act, "the design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data or as few as possible".

2) Personal data must be accurate and, where necessary, kept up to date.

An actor processing personal data must ensure that this data is accurate. The danger concerning the establishment of personal profiles based on consumer patterns is that the goods purchased may not necessarily correspond to a person's needs or habits: the purchase of a catholic bible does not mean that one is a catholic, one could be buying for someone else...It is recommended in this respect that the data subject is involved in the prior authorisation of the processing and that he is given the possibility to require that inaccurate data be modified (see below, right of rectification).

The personal data must be kept up to date. This implies that it be reviewed on a regular basis. Every reasonable step must be taken so that incomplete or inexact information be modified.

3) Personal data may only be kept for a certain period

Personal data may only be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the data were

collected and/or for which they are further processed. The data introduced by the consumer in order to purchase certain goods, may only be kept for the period necessary in order to obtain those goods and may not be stored beyond that period unless the controller has been specifically authorised to do so in the context of the profiling of his clientele.

One can question as to whether the vendor will be able to conserve data regarding individuals who enter the site but do not wish to go further and leave the site without having voluntarily entered personal data and without having purchased any goods.

4.2.4 Rights of data subject

4.2.4.1 Right to be informed

According to article 10 and 11 of the directive, there are two particular occasions when the controller must provide information to the data subject. The first is at the time of collection of personal data. The data subject must be informed at least of :

a) the identity of the controller (and his representative, if any);

b) the purpose or purposes of the processing for which the data are intended.

Further information must also be provided if "necessary in the specific circumstances to ensure a fair processing in respect of the data subject". Such information includes: the recipients or categories of recipients of the data, whether replies to questions are obligatory or voluntary and the possible consequences of failure to reply, and the existence of the data subject's right of access to and the right to rectify the data concerning him.

If personal data on consumers are collected it must be clear to them who is to use the data and what are the purposes for which the data are to be used or disclosed.

It must be pointed out that the features of a network facilitate the provision of information. In the hypothesis of data collected from the data subject, a message can appear on the screen at the beginning of the operations, providing the users with the mandatory information.

The data subject must be informed of the identity of the recipients or categories of recipients. The "recipient" is defined in article 2.g. of the Directive as any person to whom the data are disclosed whether a processor (person processing data on behalf of the controller), third party (any person other than the data subject, the controller, the processor and persons who under the direct authority of the controller or processor, are authorised to process the data), a person in a third country,.... The controller may be requested to provide information as to the identity of these persons to the data subject if deemed necessary in order to guarantee "fair processing" of the data.

The text of the Directive does not provide any indication as to what particular circumstances justify additional information being given to guarantee a "fair processing" of the data in respect to the data subject. Articles 10 and 11 merely state that the additional information must be given "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee

fair processing in respect to the data subject". The concept of "fair" processing, seems to refer to the requirement of transparency laid down in article 6.1.b. and in this respect one can consider that it is always recommended to give the data subject a maximum of information. When personal data is sent to other retailers in a consortium of companies or when a person's "wishlist-shopping cart"[50] is sent to people the customer expects to get presents from, one can expect the data subject to be informed of the recipients of this data.

The second occasion when information must be provided to the data subject is where the data have not been directly obtained from the data subject. According to article 11, he must be informed at the time the data are recorded or, if a disclosure to a third party is envisaged, no later than at the time when the data are first disclosed. Extracted data can correspond to this type of data which is not directly obtained from the data subject but which is deduced from the combination of data. If Otto or Sainsbury intend to share this type of data with each other or to transfer it to third parties, they will need to inform the data subject before disclosing the data.

The German TDDGS also provides that "the user shall be informed about the type, scope, place and purposes of collection, processing and use of his personal data. In the case of automated processing which permits subsequent identification of the user and which prepares the collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure. The content of such information shall be accessible to the user at any time"[51].

Article 11.2 provides for a derogation to the duty to inform the data subject where "in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort". This does not mean that the controller will not need to respect the principles laid down in the Directive (the purpose must be legitimate, the data must be relevant,...). It does however mean that the control by the data subject of the use of his data will be considerably reduced. One must await the adoption of the relevant national legislation to determine the exact scope of the possible exceptions to the duty to inform the data subject.

4.2.4.2 Right of Access

The Directive grants every data subject the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense, confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed.

The data subject may also obtain communication to him in an intelligible form of the data undergoing processing and any "available" information as to their sources. In the context of open networks or shopping malls as those envisaged by OTTO and Sainsbury,

[50] See 3.1.5 of P26983-D11-UCL-b1

[51] §3(5) of TDDSG

the controller will not always be in a position to provide information as to the sources of the data. He will be dispensed from giving this information if it is not "available".

The TDDSG also provides for the user's right to information about data collected and stored concerning his person. Thus according to §7 he shall be entitled at any time and free of charge to inspect such data stored by the provider. If requested by the by the user, the information can be given electronically.

4.2.4.3 Right of rectification

Following on from the right of access, article 12. 2 of the directive provides that the data subject is granted, as appropriate, the right to obtain the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data. It is up to the controller to ensure that this right is guaranteed.

The Directive further provides that the controller must notify to the third parties to whom the data have been disclosed of any rectification, erasure or blocking of the data, unless this proves impossible or involves a disproportionate effort. In the context of the sharing of information between the different actors, it is important that the notification of the rectification of the data is sent along to the different detainees of the data so that they may dispose of the most adequate and up dated information.

4.2.4.4 Right to Object

The data subject is granted the right to object on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided for by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve these data.

This right to object is granted unconditionally as regards the processing of personal data for marketing purposes. In the context of such projects as those developed by AIMedia, therefore it would appear that this right must be granted.

Furthermore, when personal data are to be disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, the data subject must be informed of this before the data are disclosed and must be offered the right to object free of charge to such disclosures or uses. The sharing of information between actors so as to establish consumer profiles, thus requires the information of the data subject prior to the disclosure of the information.

Different ways of expressing ones right to opt out could be envisaged: by ticking the appropriate box when filling in a questionnaire collecting personal data; by writing; by e-mail or by telephone.

4.2.4.5 Automated individual decisions

Article 15 states that Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is

based solely on automated processing of data intended to evaluate certain aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct,...".

This type of provision prevents decisions such as the creditworthiness of a person to be determined by an automated decision, for example, based on the geographical localisation of the person.

4.2.5 The controllers' obligations and liabilities

4.2.5.1.1 Security (article 17)

According to article 17 of the directive, the controller is required to put into place the measures so as to avoid any accidental or unlawful destruction, loss or alteration, against any unauthorised disclosure or access and against any other forms of unlawful processing[52]. The rationale of this article is that the potential danger to the data subject's right of privacy does not only emanate from the controller, who collects, stores, processes and discloses the data for his own purpose, but is also jeopardised if the data subject's data are misused by third parties who have gained access to it, whether authorised (by a processor under the instructions of the controller, for example) or unauthorised.

The security measures can be organisational (designation of a "security officer", documents handed out to the staff with precise security measures to be respected,...) or technical (computers kept under lock and key or in specially protected areas, introduction of access codes, encryption of certain documents, ...). It is left up to the controller to adopt the necessary measures. The measures are the result of the equation of three variables : the risks of the processing, the nature of the data and the state of the art and cost of implementation of the measures.

The introduction of computers and networks increase the risks, notably the threat of access to the data by unauthorised persons and the unauthorised use of the data by authorised users.

Account must be taken of the nature of the data. Processing of sensitive data (medical data, for example) will imply the requirement of a higher level of protection.

The security measures adopted will also be dependent on the state of the art and the cost of their implementation. This provision implies that the controller is under the positive obligation to keep himself informed of the new security measures available and to ensure that the level of security is adequate vis a vis the "state of the art" unless they are prohibitively expensive. A controller could be well advised to have proof that all the decisions relating to security of personal data were founded on professional expertise.

[52] "Unlawful" processing covers any processing of personal data which does not respect the national provisions adopted in accordance with the Directive. This would be the case, for example, if a controller did not provide for instructions enabling his staff to process the data (see article 16). "Unauthorised" processing or destruction covers the cases when the controller does provide for such instructions, but staff process or intentionally destroy the data without the controller's permission. "Unauthorised" access covers the cases of interferences by third parties to data which they should not have access to.

The directive also provides that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical securities measures and organisational measures governing the processing to be carried out and must ensure compliance with these measures. The carrying out of processing of personal data by another person must be governed by a contract or legal act, in writing or in other equivalent form, binding the processor to the controller and stipulating particularly that the processor shall only act on instructions from the controller and that the processor shall also be responsible for taking security measures in accordance with article 17 of the directive.

4.2.5.1.2 Notification (article 18)

The controller has a last obligation which is that of notification of automated processing to a supervisory authority. The directive does however provide for the simplification or the exemption from notification for certain types of processing operations. It is not however clear how the national laws will transpose these measures. The general idea is to largely exempt controllers and to reserve the notification procedure for special categories of processing.

4.2.5.1.3 Liability (article 23)

The Directive provides every person with a right to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question. In addition, any person who has suffered a damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

4.2.6 Conclusion

The European Union directive on the protection of individuals with regard to the processing of personal data must transposed into the legislation of the Member States by October 24th 1998. From this date on, it will become a legally binding document.

The AIMedia user profile is 'personal data'. The directive adopts a broad definition of the term 'personal data', so as to include any information relating to an identified or identifiable person. In AIMedia personal data consists in collected data (the user has answered questionnaires) and extracted data (the AIMedia deduces user characteristics based on purchase history, and statistical comparisons). This data forms a user profile, which is directly related to the customer's identity. Thus all user related data in the AIMedia user profile is considered personal data.

The personal data is processed by the 'controller'. When considering simple home-shopping, the retailer (e.g. OTTO or JS) is the controller. In the case of a mall of retailers sharing user profiles, the consortium in itself, as a separate entity, would be the controller. On the other side, the customer is know as the 'data subject'.

The controller must respect the following principles :

- **Purpose limitation principle** : personal data must be processed only for the purpose it has been collected for, i.e. personalised communication. In particular this limits the communication of the data to third parties, which can be seen as a new purpose in itself.
- **Grounds for processing of personal data** : the customer's consent can be assumed if he is clearly informed of what this data will be used for. He must also be given the option of refusing to give away personal data, and this should not be held against him. Under German law, explicit consent would be required if two retailers were to share user profiling information, unless data is anonymised.
- **Prohibition of processing of sensitive data** : it is safer to get sensitive data (political opinions, ethnic origin, health, sex life, religious beliefs) trough explicit questionnaires.
- **Data quality** : data must be adequate. It must be tightly linked to its use. In the case of offering a more personalised service (as for AIMedia), the criteria for adequacy would allow the processing of more data than in traditional shopping. Data must also be accurate. Purchase behaviour does not necessarily reflect personal needs or habits. Data can only be kept a certain time.

The customer has the following rights :

- **Right to be informed** : the customer must know who is to use the data and what are the purposes the data will be used or disclosed. in the case of a mall of retailers the 'recipients' of the data must be clear. The customer must also be informed each time his profile is transferred to third parties.
- **Right of access** : the customer has the right to know whether personal data is being processed by the retailer.
- **Right of rectification** : the customer will be able to correct incomplete or inaccurate data.
- **Right to object** : the customer should be allowed to opt out or to refuse the disclosure of personal data to third parties.

The controller has the following obligations and liabilities :

- **Security** : the customer's right of privacy must be insured by securing the retailer's host and transactions when sending information over the network.
- **Notification** : Simplification or exemptions will be specified in national legislation.
- **Liability** : every person has a right to a judicial remedy for any breach in the applicable rights regarding personal data processing.

4.3 Conclusion on legal aspects

Respecting the European directives on advertising and personal data protection therefore implies for AIMedia to implement the following requirements :

- We need to have a clear message to the users when offering the AIMedia agents. The message communication should be seen as a mean to insure confidence in the system.

- Prompts (offers, advice, etc...) should be seen as a new service which requires personal data.
- When data is collected through a questionnaire a clear message should explain what this data will be used for. If new fields are asked for, it should be explained which new service this provides.
- It is the retailer's responsibility to insure sufficient protection of the personal data through security policies, both organisational and technical.

The following design issues should moreover be addressed :

- The user profile variables do not have all the same status : some are obtained through the answers to a questionnaire. They are public but could be shared by all retailers, or could be specific to some (eg. I want to buy my fish at Sainsbury's - so I specify my preferences only for this store). Some variables are compiled from purchase history (eg. Average spend per week) or some are extracted or inferred variables from a more global statistical analysis, a clear access right policy needs to be defined.
- The user interface should implement a way for the user to keep control of his profile, through a profile manager. This must include opting in and opting out which the user would monitor interactively.
- A special care should be taken when sharing information between several retailers : an explicit consent can be asked for in the case of an electronic mall of retailers. But when dealing with mobile agents that 'go shopping' on the net, it is not possible to know in advance the list of targets, and to ask for permission to the user each time the mobile agent reaches a new (possibly) interesting site. Should all variables be public ? Should the visited retailer be permitted to record the agent's visit ?

As we have seen sufficient data protection should be granted by the retailer through reasonable technical and organisational means. In the following sections we investigate these means and we explain how we intend to integrate these technologies into the AIMedia secure advertising framework.

ANNEX 2 : Assistance to AIMEDIA on Digital Signature

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

AIMEDIA ASSISTANCE

CONTRACT LAW - DIGITAL SIGNATURE

UIB

DIGITAL SIGNATURE

ECLIP-UIB
AIMEDIA

In our opinion two are the points related to digital signature that may arise legal issues.

AIMEDIA will create a virtual market place, in which may exist contractual relations between consumers and enterprises (Consumer Law), between enterprises (Commercial Law) and between individuals (Civil Law).

1. - Validity of electronic contracting.

The AI MEDIA virtual market place need to make agreements by electronic means (without using the traditional writing documents) using the digital signature technical.
One of the points that have to be solved is the equivalence of the digital signature in a electronic contract to the signature of a writing contract, because some States request for contracting between consumers and retailers or service providers (and for some specific contracts), the writing form for validity. In this cases, if digital signature can not be equivalent to writing signature, contracts made by electronic means will not be valid.

When the buyer or the person who receives the service is an enterprise, rule the principle of free form. Contractors may choose the form they consider more convenient in order to celebrate their contracts, so electronic contracts do not have any trouble for validity from this perspective.

It is the same when the agreement is between consumers (individuals), as generally civil law establishes the principle of free form. Only in some specific cases law establishes the requirement of a writing form for the validity of contracts, (it can be in function of the object, or the price).

2. - Electronic documents validity and efficiency in Court.

Solved the validity problem, the second step will be to determinate if electronic documents can be accepted by a jurisdictional court. (It would be necessary to solve if free evidence exist or if the presentation of means of evidence is limited)

In Great Britain, after the 1995 amendment ("Civil Evidence Act" 1995) seems that there are no difficulties to admit electronic documents as evidence. Regarding to Germany, after the approval of the 1997 Law about digital signature regulation although there is not an express equivalence between writing documents and electronic documents, the doctrine usually says they are equivalent.

Once resolved their admission in a judicial process as documents (or as evidence), it is necessary to determinate its efficiency, this means its credibility or reliability.

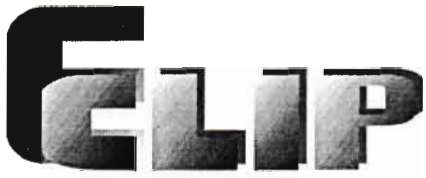
The efficiency of an electronic document, depends, generally, from its reliability (this means from its integrity). A document that may be modified from anyone will lack from efficiency in a Court. Therefore, in first place, we need a document that can not be modified, electronic documents should live evidence of who is the drawer and who the receiver and also of its content.
This reliability can be obtained by using digital signature, which guarantees the integrity of the message, and by the intervention from an independent third who certify the key ownership used to send the message. (The third guarantee the authenticity of the message)
This point seem to be solved by AIMEDIA with its constitution like a independent third and using the adequate technology which allows the guarantee of the authenticity and integrity of the electronic message.

If AIMEDIA decided to participate in the market (p.EG. selling their own product), then will have the problem because the result will be that the certification authority will be an interested part into the market, so that will suppose that a contracting part is also responsible from keys and certificates, so that one of the contracting parts will controls the hole security system (this will have repercussion in credibility of the hole system in regards of integrity and authenticity). This in a judicial process, will be defective evidence because of the interested party.

Another problem that will be necessary to solve is the one concerning to the transmission and reception evidence of the message.
It is necessary that AIMEDIA, or a third party certify that the message has been sent and received, if not the receptor may simple asseverate that he have not get the message.

ANNEX 3 : Assistance to AIMEDIA on International Private Law

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)



Electronic Commerce Legal Issues Platform

AIMedia – Issues of private international law

NRCCL contribution to assistance

Morten Foss and Peter Lenda

INDEX

1. INTRODUCTION

1.1. Introductory remarks

The establishment of a web shop may create several advantages for the retailer. One is the simplification of reaching out to customers located in foreign countries. If a French retailer offers his products on the Internet, it will be equally easy for a Swede as for a French person to access the web page, find out what it has to offer, and eventually order some of the products. Consequently, it is easy to imagine that there may arise cross-border conflicts, that is, legal disputes which involves parties situated in different countries. An action[1] committed on the Internet, whether in form of the collecting of personal data, advertisement of products etc., might be in accordance with the law of one country at the same time as it violates the law of another country. Which country's court shall have the competence to adjudicate, and which country's law shall form the basis for the solution of the material question? These are the issues that are going to be dealt with in the following chapters.

1.2. General delimitations

The subject of this report is to sort out the questions of jurisdiction and choice of law. The framework of the project will not allow a profound analysis, whereas the report will have to concentrate upon identifying some of the more important questions, and try to point out possible solutions to these. Consequently, we will analyse three main fields which are relevant for AIMEDIA project, i.e. data protection, advertising and liability on the basis of loss suffered due to misleading information. Still, in this report one will have to operate with certain delimitations. It is therefore assumed that:

- It is presumed that the legal disputes are of an international character, see under section 2.
- If the legal disputes are qualified to be a matter of public law, special questions arise in accordance with the application of the rules governing the questions of jurisdiction, choice of law and enforcement. In the following it will therefore be assumed that the legal disputes in question, are a matter of private law. However, this assumption will be suspended to some extent in discussing advertisements on the Internet.
- Questions of consumer rights and product liability will not be treated.
- It is presumed that the legal disputes takes place between parties domiciled within the borders of the EC or the ECCA-states.
- It is presumed that the defendant of the legal dispute is the web shop's responsible institution. Third party conflicts (e.g. liability of intermediaries) fall outside the treatment.
- It is presumed that the objects, which are to be distributed, are assumed to be ordinary merchandise in the form of tangibles. The sale of services will not be considered.

---

[1] The action in question might be generated both manually or by a computer.

2. AN INTRODUCTION TO PRIVATE INTERNATIONAL LAW

2.1. The problem

When two parties enter into a legal conflict, the usual step is to ask the courts for help. In a normal situation this does not cause any problems. Two neighbours will go to their local court, and this court will use its own rules. However, a problem arises when the two parties do not reside in the same country, or the problem has connections to more than one country.

The problem is defined by a «foreign element»[2], that is not the one of the court. It is in these cases one has to apply the rules of private international law.

Private international law basically rules over matters between private parties and not when there is a public element involved.[3]

In the following we will review some general points of private international law. This is a way of introducing this field of law and the questions surrounding it. First of all, the main questions raised by private international law of jurisdiction and choice of law are discussed. Afterwards we will canvass some of the topics around private international law, like (2.3) the place of private international law in the internal law, (2.4) the name used on the field, (2.5) regulations, (2.6) what to do in case of lack of regulations in this field, by giving an example, (2.7) *renvoi*, (2.8) the limitations of private international law, and finally (2.9-2.11) private international law and cyberspace.

2.2. The main questions

The judges in these cases must, before solving the material case itself, determine two major questions. First of all the court must decide whether it has jurisdiction[4] over the case; i.e. if the parties in question can bring this case into the court. Secondly it must determine what rules to apply to this case. This is a choice of law, and not the application of certain rules to the case. The foreign element in this case gives the court the choice between more than one set of rules. A final question that has importance in interlegal law, is the question of recognition and enforcement. In this report we have chosen not to deal with this problem, mainly because it is often solved under the jurisdiction issue.

To be more practical, if two parties goes to court to solve a legal problem that has a foreign element, the first task of the court is to determine if it has jurisdiction over the parties – which means whether they can render a valid decision with respect to the legal problem. If this is so, the next step will be to decide which law governs the case, i.e. the choice of law. This part consist of several elements. First of all there has to be a classification of the case. It is of great importance if the case is classified as contractual law rather than the law of procedure. When this is done, the court must see if there are some regulations dealing with this problem. If there are not, one has to apply the basic rules of private international law. The result of this will be to determine which country's substantive law governs the question. Once this law has been chosen, the court must primarily use this law to decide on the case. Unfortunately this is not always the end of the process. There may be mandatory rules in the

---

2 Joachim Benno; *Consumer purchases through telecommunications in Europe*, Complex 4/93 Tano (Oslo 1993), p. 21

3 In some cases there will be overlap between private and public law. This overlap is normally not an issue in private international law.

4 Jurisdiction is not always considered to be a part of the private international law, but of the internal procedure law of the country. In these countries, like Sweden, private international law is considered to only consist of the choice of law.

country of the court, which collide with the *lex causae*[5]. In some cases this leads to the use of *ordre public*[6], which requires that other rules be applied. The rules may be either secondary rules of the *lex causae* that are not incompatible with the rules of the court, or rules of *lex fori*[7].

2.3. A part of each country's internal law

It is important to note that even though the name suggests that the rules are international, and valid for several countries, this is not so. Most countries have a private international law, which is a part of their own legal system. And when a case has a foreign element, each court should, even ex officio, use these rules. Further down we will come back to the fact that some parts of the world have harmonised some of these rules.

Another important point is that even if the court does apply its own private international law, and then chooses another legal system, there are still some rules of its own that a court will use. Without going any further, this is the court's own rules of procedure and evidence.

2.4. The name of the field

In some countries, the use of the term «private international law» is not common. Instead the term «conflicts of law» is used. This term is usually used by American authors because the conflicts of law in the USA has not been a conflict between national laws, but between the laws of the different states (often called intranational law).

As this report is mainly addresses European conflicts, the term "private international law" will be used in this report.

2.5. Regulations

On the national level, the field of private international law generally has not been regulated in great detail. Certainly there are elements of private international law in several statutes of any countries, or the existing rules are used by analogy. On the other hand, the courts have often filled non-regulated fields. Therefore many of the rules of each country's private international rules are non-written, but they are still valid.

On the international level, there are several efforts to harmonise this field. Examples are the Brussels, Lugano, Hague and Rome Conventions, or the European Convention on Transfrontier Television. Inside the EU, there has been done a great deal of work on harmonising several fields of law. An example is the Directive on data protection. As for the Rome Convention on the law applicable to contractual obligations, this has recently been more or less adopted as formal law by Switzerland. Even so it must be said that these regulations are mostly European. This means that there are great uncertainties when a case involves someone from outside this region.

As for the Lugano and Brussels Conventions, they are similar conventions, solving the jurisdiction in most Western Europe,[8] for cases dealing with private and commercial matters.

---

5 The law of the case

6 Public policy of ethical and social character.

7 The law of the court (forum).

8 The Brussels Convention solves jurisdiction inside the EU, while the Lugano Convention covers the jurisdiction between the EU-countries and some of the EFTA-countries (Norway and Iceland, in addition also Switzerland).

The conventions also solve the problems of these cases concerning recognition and enforcement.[9]

The Rome Convention on the law applicable to contractual obligations does solve the problem of what law governs a contractual obligation between two parties. The principal rule is that the parties have the freedom to choose the applicable law.[10] In absence of such a choice, the rule is to choose the law of the country with which the contract is most closely connected.[11]

The regulations do not always give a private international law solution, but they can also be considered to be a kind of unification of substantive law, especially in the EU. In such situations the conventions or Directives main purpose is to avoid conflict.

2.6. What to do, if in lack of regulations: Methods of solution

If one operates only inside the EU, it is not unlikely that one will find a solution in a regulated law or convention. If not, one will have to apply the general principles of international private law. By this we mean that the court in question does not have any international or European treaties or regulations on which to rely, or any clear national rules to apply. The best explanation is an example.[12] For electronic commerce, the most important field is the one of contractual obligations. This is because the parties in question mainly will try to conclude a transaction on the Internet. One could imagine that there are no regulations in this field, even if the Rome Convention probably will do so. For example:

Assume a Norwegian living in Denmark, contracted in Madrid with a Frenchman (living in Belgium). Assume further that the Norwegian delivered the goods in Germany and has his place of commerce in Sweden. There are many different possibilities as to what law governs this case. Imagine that a court has decided that it has jurisdiction over the parties and that this is a case with a foreign element, one could have these possibilities for the law governing the contract:

- The law of the domicile of the seller (Danish law)
- The domicile of the buyer (Belgium law)
- The law of the country where the contract was finished (Spanish law)
- The law of the country where the contract was fulfilled (German law)
- The law of the place of commerce of the seller (Swedish law)
- *Lex fori* (if the case is brought into a court in another countries)
- The law of the citizenship of the seller (Norwegian law)
- The law of the citizenship of the buyer (French law)
- The law where the contract has it's closest connection.
- The party autonomy, if it is accepted and the parties have chosen a law.[13]

As for this report, the most important of these solutions will later be the one of the closest connection. In contrast to the method of a ''single connection'', which could be solutions like the law of the place where the contract was made, the place of performance or the law

---

9 There are exceptions to the private and commercial matters in art.1(2).

10 Rome Convention art.3.

11 Rome Convention art.4(1).

12 The example is built upon an example taken from the most excellent book by Nikolaus Gjelsvik: *Millomfolkeleg privatrett*. p. 213.

13 This is the solution of the Rome Convention art. 2.

according to the domicile or nationality of either the seller or buyer. The closest connection method will be discussed under the section 4.3: Choice of law and liability for economical damage due to misleading information, together with some of the other solutions. In situations where the parties have not made an explicit choice of law in contract, the court might apply the closest connection method. This method implies that all the connecting elements to the contract and the parties are brought together and weighted against each other in order to find the law of the country where the case has its natural seat. For the court, the problem is the weighing of these so-called connections. Because these connections are not stable from case to case, this method is flexible, but unpredictable for the parties.

Looking back at the different solutions, one can see there is a large variety of solutions to a case where there are no direct regulations. In such a case, the court will, if it adheres to private international law, have to look at the different solutions. The next step will be to look at the different arguments. We will here look at different important arguments, but the list is not complete.

First, it is important to look at the *predictability* of the law chosen for the parties. A good solution gives every party the possibility to predict the law chosen in the actual case. As an example, the solution of closest connection gives the lowest predictability if there are no directions for what arguments will be used for deciding the closest connection.[14] On the other hand a solution like the closest connection will most likely reduce the forum shopping-effect: The parties will not be able to escape the obvious law of their legal problem.

But there are other arguments that have to be discussed. The possibility for a contributing to *international unity* is important. This means that if this is a solution several countries have adopted, it is probable that other states will use and accept it. And again this reduces the possibility for forum shopping. This leads to another argument, the argument of *acceptance*. It is wise to choose a solution that other countries will accept, especially considering the law of the country of the foreign element. This again leads to the argument of *execution*.

These arguments are not the only one to take into consideration; they are only arguments of principle. In practice the court of jurisdiction will apply *lex fori*[15] to many issues. This so-called "homeward trend",[16] is often used when the court is not too familiar with the private international law. It is also important to note that the court often will consider having sovereignty over the case and therefore applying *lex fori* automatically.

Finally, all arguments taken into consideration, one will have to use one solution. Step two will then be to identify the law applicable to the case; but then again, there are other limits.

2.7. Renvoi

Renvoi is a very special part of private international law. It can come into action if the law chosen is not the one of the court. In such a case it is possible that the law chosen is a law of a country where this county's private international law chooses our *lex fori* as *lex causae*. In such a case, the question is whether to accept this «*renvoi*» or to use the substantive law of this country. If one chooses the first one could end up with a situation where the laws bounce back and forth[17]. In French law this argument is called *argument de*

---

[14] See article by Helge J. Thue in TfR 1965 p.587-610.

[15] The law of the court

[16] Term often used in the USA

[17] This is a not likeable argument against *renvoi* because it does not take into consideration that the case is in one court and it is this court that will accept or refuse the *renvoi*.

la raquette[18]. On the other hand *renvoi* is not accepted in the Rome Convention – applicable to contracts- art. 15. Among most European countries *renvoi* is a known question that has nor been abolished, but a choice of law means normally a choice of substantive law. In English law this is the normal idea[19]. The question of *renvoi* will not be any further pursued in this report.

2.8. The limits of private international law – ordre public

Private international law has its limits. First, because all matters of public law are held excluded. Second, there are limits both inside private international law and in other national law fields. The latter can be referred to as the mandatory rules in the law of each country. The boundaries to mandatory rules versus the choice of a law in private international law must be discussed separately in each single case. In cases of consumer protection, the 1980 Rome Convention on the law applicable to contractual obligations has rules on mandatory rules in art. 7, while the *ordre public* rule is stated in art. 16, indicating that these two question must be kept apart. The boundaries to mandatory rules is a part of the choice of law process, while *ordre public* is a process that takes place *after* the choice of law has been made. As for mandatory rules, this report does not pursue this question any further.

What is *ordre public*? Once a *lex causae* is chosen, this is not the end of the matter if the *lex causae* different from *lex fori*. Considering that the law chosen is not *lex fori*, there are possibilities that the court will not accept the application of this law in question because the application of the substantive law will be incompatible with the public policy of the forum. An example of an *ordre public*-rule is the Rome Convention art.16:

> ''The application of a rule of the law of any country specified by this Convention may be refused only if such application is manifestly incompatible with the public policy ('ordre public') of the forum ''

For the rule of *ordre public* to come into action, it is the application of the *lex causae*, i.e. the foreign rule, must be *manifestly incompatible* with the public policy of the forum. For the foreign rule to be *manifestly* incompatible, requires that the application of this rule lead to the exclusion of the rule. If the *lex causae* has provisions that are incompatible with the court public policy, the rule of *ordre public* can not be applied. The qualification of the rule to be incompatible with the public policy is not easy to define. On the other side there are strong suggestions in the European theory that the incompatibility must be between the ethical and social norms of *lex fori* and *lex causae*. In addition these differences between these ethical and social norms must be strong. We do not pursue this matter any further.

Finally it must be noted that if the court applies the rule of *ordre public*, the question is what rules shall then be applied. The choice lies between *lex fori* and secondary rules of the foreign law.[20] Many courts will as a result of *ordre public* collisions apply *lex fori*, mainly to avoid the problem. But how this is done differs. In some cases the court will apply what in Norwegian theory[21] is called *positive ordre public*, meaning that national rules of the court have an ethical or a social norm that can not be in breach of any foreign law, and therefore *lex fori* will apply.

---

18 Gaarder: *Innføring i International privatrett* Universitetsforlaget 1993 (2nd ed.), p.85

19 Cheshire&North's: *Private International law* (11th ed.) p. 72

20 It could also be that the applicable law chosen, is secondary rule, and one would then have to look at the primary rule of the law.

21 Gaarder *l.c.* p.48

As to this report, we would like to note that in private international law this field is referred to as *ordre public* or public policy in Anglo-American countries. In this report the term *ordre public* will be preferred.

2.9. The application of this field to cyberspace

Unfortunately it is a well-known fact that the courts often disregard private international law. First, the parties often do not have the means to get acquainted with a foreign law by hiring a specialist from a foreign country. Second, the court itself prefers to use its own *lex fori* because this is the law known and because the lack of time does not allow the judge to use more time than necessary on the case. Therefore the question for the future is how the courts in Europe will use the ''instrument of private international law'' on the legal questions that raises from the use of Internet as a commercial marketplace. It is at this point the interesting questions start.

2.10. The international aspect of the Internet

What is considered to be an international case when it comes to cyberspace? When entering cyberspace things change because any contact made over the Internet can be "international". At no point is it sure that if you exchange email with your closest neighbour, this email will go directly to him – it may go across the world before reaching him. This is why the foreign element might be present at all times when using the Internet. Now, if you exchange emails with your neighbour about buying his Rolex, the court will most likely regard this as a national matter. On the other hand, if your neighbour places an advertisement offering his Rolex for sale on the Internet, it is not sure that you will be able to identify him. At this point the matters seems more international, and the court should consider if the case should be solved using private international law. We will not take this argument any further, but it may be a point to argue in front of a court.

2.11. Some points of interest concerning Internet and law

The laws applicable in the analogue world may not be the same as in the digital world. This is important to understand with respect to the question of applicable law. Not only is there is no direct contact between two contracting parties, but also the identification of these parties is not always possible. Many of the laws and acts related to international trade are based on the presumption of direct contact between the parties, and that the object of the trade is physical objects. When using the Internet this is not as obvious. What is contracted, may be sold and sent over the Internet.[22] This again raises problems of intellectual property rights, which will not be addressed in this report.[23]

In this report we will try to examine the main issues related to private international law and web-shops. This examination will mainly consist of looking at the present regulations, and whether they are applicable to the issues in question. For some issues there may be some regulations developed especially for a digital environment, which then will be applicable. On the other hand there might be issues where it will not be possible to apply current regulations.

---

[22] There are great advantages doing so. Notably the expenses and the wrapping, i.e. buying music over the Internet in the future will not consist presume the purchase of a physical object like a CD, but the transfer of a file over the Internet.

[23] Jon Bing: *The identification of applicable law and liability with the regard to the use of protected material in the digital context* (E-CLIP draft report).

Here the question will be what alternative solutions can be found. The first solution is to consider if the traditional regulations can be adapted. This will in general mean to try to identify the parties in question and their places of attachment. If this is not possible, we will have to rely on the traditional private international law, and to explore the consequences of their possible application. However, at this point we will be arguing mainly on the basis of legal policies.

3. JURISDICTION

3.1. Introduction

When a legal dispute enters the court, the court will have to decide whether it has the competence to adjudicate in this specific case. Concerning courts within the area of the EC and the ECCA-area there are two conventions, which in many cases will provide a solution to the questions; the Brussels- and the Lugano Conventions. All the member states of the EC have become parties to the Brussels Convention of 27 September1968. Furthermore, all the ECCA-states (with the exception of Liechtenstein) have become parties to the Lugano Convention of 16 September1988, which for our purposes may be seen as identical to the Brussels Convention with respect the material content. The two conventions will be treated as one in the following.[24]

The conventions only provide solutions for cross-border disputes concerning "civil and commercial matters",[25] that means legal disputes as part of *private law*. In the ruling of the EC-court *LTU v Eurocontrol,*[26] it is stated that essential for the qualification is the character of "the legal relationships between the parties to the action of the subject matter of the action". In other words, it is only in situations where a public authority has exercised public authority, that the provisions is inapplicable. The qualification of whether a legal relationship is to be deemed a matter of public or private law, is to be determined on the basis of an autonomous interpretation of the Convention, where respect shall be paid to the purpose and the structure of the Convention, and also the shared principles that can be extracted from the legal systems of the parties to the Convention.

As concerning the enforcement of advertisement legislation, this typically will be considered a matter of public law, and thereby fall outside the scope of the conventions. The treatment of the jurisdiction as it comes to the questions concerning the enforcement of advertisement legislation, therefore will be dealt with in a separate point, see sect. 3.3.

3.2. *Jurisdiction in matters of private law*

3.2.1. The point of departure

As a point of departure, the defendant is to be sued in the courts of that state where the defendant has its seat. In order to determine the seat, the court shall apply its own rules of

---

24 Reference to articles in the following, will be based upon the provisions laid down in the Brussels Convention.

25 Art. 1 (1)

26 Decision of October 14th, 1976 in Case 29/76, LTU v Eurocontrol [1976] ECR 1976; Concerning the Brussels Convention.

private international law.[27] In our context, the provision does not generate any special problems, and consequently further analysis can be avoided.

3.2.2. Special provisions

In certain cases, alternative provisions may determine the jurisdiction. The most interesting in our context are:

a. Matters relating to a contract, art. 5 (1)
b. Matters relating to tort, art. 5 (3)

The provisions are alternatives to the provisions in art. 2, which implies that the plaintiff can decide whether to sue in the country of the defendant or in courts of the country that follows from the rules laid down in the special provisions.[28]

Matters relating to a contract

In matters relating to a contract, art. 5 (1) states that a person can be sued "in the courts for the performance of the obligation in question". The EC-court has decided that the relevant obligation does not necessarily have to be the characteristically performance of the contract (typically: the merchandise to be delivered). A contractual relationship will nearly in all cases consist of several obligations of different character. This may lead to the fact that there might be operated with several *fora solutionis* to the same contract.

In determining what are to be considered as relevant obligations, the decision of the EC-court in *De Bloos v Bouyer*[29] must be considered. The decision makes a distinction between primary and secondary obligations of the contract. The secondary obligations are defined as having the character of sanctions, which replace ordinary obligations of the contract (the qualification is done on the basis of national law). It is only the primary obligations that are relevant for determining the jurisdiction. The decision has been criticised, but nevertheless must be seen as an expression of contemporary law, as the decision has been followed up by the court in later cases, also the wording of the provision supports the result of the decision.

It might be that the defendant, in the contract between the parties, has obliged himself to handle the collected or extracted personal data in a specific manner. Given that these obligations are defaulted, it may be argued that the obligation in question is the basis of the dispute, and that the place where this obligation is to be performed can be chosen as an alternative venue. Similar considerations can be made if the defendant in the contract has guaranteed the accuracy of the information provided, and the customer suffers an economic loss because the information proves to be incorrect. It is likely that a court will hold that obligations like those mentioned above must be qualified as a primary obligation. Consequently, the courts of the country where the obligation in question is to be performed will be competent to adjudicate.

The problem therefore consists of determining at what place obligations like those mentioned above are to be performed. The solution will specifically depend on whether the place of the performance are agreed upon by the parties or not.

---

27 Art 53 (1)
28 Provided that this will be a different jurisdiction
29 *De Bloos v Bouyer* , 1976 ECR 1497

If the parties have agreed upon the place of performance of the obligations in question, the parties are bound by the agreement.[30]

Given that a valid agreement between the parties does not exist, the Convention does not provide any solutions to the problem in our context. There are likely to exist national differences when it comes to determining what place is to be considered the place of performance, and accordingly it will be impossible to give a definitive answer to what is likely to be the result in an actual case. One will therefore have to calculate with the risk that obligations like the one mentioned, can be argued to have universal relevance. That would mean that their compliance not only would have to take place in the countries of the seller and buyer, but potentially also in all other countries in the world. If such obligations are violated on the Internet, one will easily submit one self to the situation where the courts of practically every nation in the world will have the potential to adjudicate.

Matters relating to tort

As for matters relating to tort, the courts of the country for the place where "the harmful event occurred", will have jurisdiction, art. 5 (3). A tort is a wrongful act or omission for which damages can be obtained by the person wronged, other than a wrong that is only a breach of contract. In the AIMEDIA scenario, a tort can consist of a violation of data protection principles for which the concerned person can bring a suit, or a violation of advertisements regulation where a competitor or a consumer can feel wronged.
The EU-court has stated that one has to establish an autonomous understanding in the interpretation of the expression "the harmful event occurred".[31] Furthermore the EC-court has interpreted the expression to also include the place where the effects of the harmful event took place, see *Bier v Mines de Potasse d'Alsace.*[32] In the case *Sheville v Presse Alliance*[33] there is given a general definition on what might be seen as the place where the effects of the harmful event took place. This is the place where the harmful event has caused damage to the injured party. These guidelines must be presumed to have relevance also when it comes to actions committed on the Internet. In the determination of the venue, one shall not include consequential damages or loss in the consideration. This is stated in the decision *Dumez Batiment v Hessische Landesbank.*[34]

It must therefore be presumed that contemporary law holds that in every country where the injured party has suffered loss due to the harmful event, the courts will probably have competence to adjudicate.[35] This is also goes for the situations where the responsible action was committed in the context of the Internet. In the doctrine it is presumed that also loss of a non-economic nature, like compensation for damage of a non-economic nature or compensation for defamatory statements etc., sets out the right to adjudicate in accordance to art. 5 (3)[36].

Concerning violations of intellectual property rights committed on the Internet, it has been stated by some authors that the competent countries must be limited to only incorporate those countries to which, on the basis of an objective assessment, it seems likely that the

---

30 *Zelger v Salinitri I,* 1980 ECR.

31 *Marinari v Lloyds Bank,* 1995 ECR 1-49.

32 *Bier v Mines de Potasse d'Alsace,* 1976 ECR 1735

33 *Sheville v Presse Alliance, 1995 ECR*

34 *Dumez Batiment v Hessische Landesbank,* 1990 ECR 1-49.

35 However, an important limitation lies in the fact that it is only possible to seek compensation for damages which didn't occur within the territory of the country.

36 *Stein Rognlien Luganokonvensjonen – norsk kommentarutgave* p. 147

copyrighted material will be downloaded.[37] According to this consideration it will only be the courts which have their judicial district within the "targeted area" that have jurisdiction. It might be questioned whether a similar limitation must be applied also for other types of infringements. The question will not be pursued here since it is doubtful whether the above listed presumption can be seen as an expression of current law. However, there might be reasons to note that if the presumption is to be followed by the courts, it is likely that similar considerations would apply also to other kinds of infringements. The condition for applying the same considerations is of course that it is possible to stake out a specific "target area".

3.3. Jurisdiction in legal disputes concerning claimed violations of advertisement regulation

With respect to the application of the regulation of advertisements, it is mentioned above that this typically will be considered as being part of public law. The reason is that the advertisement regulations are enforced by public administration. The legal dispute therefore lies outside the scope of the conventions. The question that emerges is which rules will then apply in determining the jurisdiction.

It is an acknowledged principle that when dealing with public law a state can only assume jurisdiction if the assumed infringing event falls within the scope of national legislation. One will therefore have to interpret the application of every single national regulation. Such an analysis exceeds the basis of this report, and consequently will not be undertaken.

However, there are reasons to believe that an essential criterion will be whether the advertisement has taken place within the *territory* of the country. For these reasons, the question will be how such a criterion is to be applied for advertisement on the Internet.

At the first glance this may seem trivial. Advertisements on web pages are capable of being viewed in all European countries, and one might therefore say that the medium, which is chosen to display the advertisements, should not determine the application of legal rules. However, the way that the advertisement is transmitted on the Internet may create problems. This is because the retailer himself does not commit any *active* actions in order to distribute the advertisement to a certain country. It is the end-user who makes the connection to a database containing the web page in question, and thereby initiates the transmission, so that he finally will have the advertisement displayed at his own screen. Is it then, under these circumstances, plausible to state that the advertising is taking place within the territory of the country where the end-user is located?

Imagine that a Swedish court claims that their national legislation governing advertisement is violated by an English retailer who has his database on a server geographically located in United Kingdom. It might then be argued that the advertisement is taking place on the server located in United Kingdom, and therefore will not fall within the scope of the Swedish regulations.[38] The fact that a Swede through establishing a connecting to the database has the commercial displayed on his own screen, cannot be the retailer's problem as long as the retailer in question has not made any active attempts to transmit the commercial to Sweden. One might say that the situation will have to be placed on equal footings with situations where a Swede during a vacation in London buys a magazine containing advertisements which are forbidden by Swedish legislation and brings the magazine back to Sweden.

However, it is not certain whether such a formal consideration will be accepted by a court. It may be maintained that when a retailer chooses to advertise his products on the Internet, he

---

37 Andreas Fuglesang and Georg Krogh *"Internett og jurisdiksjon"*, 1998 (ms)

38 *Joachim Benno* "Consumer Purchases through Telecommunications in Europe", Complex 4/93 Tano (Oslo 1993).

must be aware of the potential of the advertisement being displayed on all screens connected to the Internet, and that the reality therefore is a world-wide promotion of his product. This was probably also the idea of choosing exactly this specific medium. It may therefore seem inconsistent that retailers who utilise the Internet as a medium to promote their products shall be put in a more favourable position than the ones that utilise more traditional media for the promotion.

It is uncertain how the question will be solved. It is likely that the way the national courts solve the problem will depend greatly on to what extent they feel obliged to lay down a strict understanding of the wording of the provisions.

4. CHOICE OF LAW

4.1. Data protection and choice of law

4.1.1. Introduction

Data protection will be in the future, as now, an important issue in a digital society. Increasingly personal data is being stored on computers that are connected to other computers. The possibility for people to access this information across jurisdictional borders is also increasing. This, in turn, increases in the potential for choice-of-law issues arising with respect to regulation of the information processing concerned.

The following analysis rests on several presumptions. First, we presume there is an issue involved which has a certain international, or foreign, element, thus allowing the issue to be considered a question of private international law. An example is a Web-shop, which collects data about customers who are not situated in the same country as the owner of the Web-shop.

Second, we presume that the matter is of a private character. By this we mean that the parties presenting themselves to the court do not include government agencies.

Third, we presume that the matter occurs within the geographical area of the EU/EFTA countries that have signed the Lugano and Brussels Conventions.

Fourth, we presume that the parties have been identified, and that the transactions between the parties did not occur anonymously.

Finally, we presume that the aim of this analysis is to allow the owner of the Web-shop to be able to predict more precisely which law will regulate the processing of data about his customers.

4.1.2. The regulation of this field inside certain areas

Every EU/EFTA state has enacted data protection legislation. Furthermore, the EU has adopted a Directive on data protection (Directive 95/46/EC – hereinafter abbreviated "EC-DPD") which is aimed at harmonising data protection regimes inside the EU. This Directive will also be highly influential for the development of data protection law in EEA states that are not members of the EU – i.e., Norway and Iceland – especially once the Directive is formally incorporated in the EEA Agreement.

4.1.3. The Directive's impact on Internet-shopping

The EU DPD applies to "the processing of personal data wholly or partly automatic means, and to the processing otherwise than by automatic means of personal data which form part of

a filing system or are intended to form part of a filing system" (art. 3(1)). There are certain delimitations to the applicability of the Directive laid down in art. 3(2) but these are not relevant to the analysis here.

The Directive will apply to all types of web-shops, like those of Otto Versand and Sainsbury's, when these collect and further process data that is "personal" pursuant to art. 2(a) of the Directive. Art. 2(a) defines what is "personal data" as follows:

> 'personal data' shall mean any information relating to an identified or identifiable natural person ("data subject"); directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; ....'

In light of this definition, it is possible that the information stored by a cookie mechanism could be considered as "personal", though this is a point of debate. For further discussion of this issue, see the part of the deliverable 13 drafted by Sophie Louveaux from the CRID.[39]

4.1.4. The law applicable to the processing of data

The next point is to identify the law applicable to the handling of the database and the data concerned. According to art. 4(1)(a) of the Directive:

> 'Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where ... the processing is carried out in the context of the activities of an establishment of a controller on the territory of the Member State ...'

As to who is the controller, this is defined by art. 2(d) as:

> 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data ...'

This means that the responsibility for observing the rules laid down in data protection law is given to those actors that control the means and purposes of the processing of data on other persons. Note that art. 2(d) envisages that there can be more than one controller per data-processing operation. Further, it is factual control over, not possession of, the data, which is the main criterion for being a controller.

Of decisive importance for working out which law is to be applied to a given data-processing operation, is the meaning of the term "establishment" in art. 4(1)(a) of the Directive. Some light is cast on the meaning of the term in recital 19, which states:

> 'Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on territory of several Member States, particularly by means of subsidiaries, he must ensure,

---

[39] See also L A Bygrave & K Koeman: *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems* (Amsterdam: Institute for Information Law, 1998), p. 13. The report is also available via URL <http://www.imprimatur.alcs.co.uk>.

in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities; ...'

At this point, the principal rule must be said to be clear in the case where we have one controller with only one place of establishment: the applicable law will be the law of that place of establishment. This means that if a controller has headquarters in country A, the data protection law of country A will apply.

Problems arise when the controller is established in several jurisdictions. We will address these problems below.

4.1.5. Problems of the Directive

In this section, we will look at the problems resulting from a situation in which the controller is established in multiple jurisdictions. Second, we will consider the issue as to whether data mining can be considered as involving a contract between the controller and its counterpart. Finally we will look into the problem of *ordre public*[40].

Problem 1: The controller has more than one place of establishment

As we have seen in sect. 4.2.4, it is quite clear that an "establishment" may include subsidiaries, branch offices, and perhaps also agents or similar representation. This means that if the controller has a main office in one country, and several branches in some other countries, different laws will be applicable to a single data-processing operation that extends across borders.

To be more specific, we can imagine one controller, A, situated in country A, exchanging information with its sub-branch, B, in country B. The collection (or mining) of this information can take place from almost any country. If there is no exchange of information, the data processing in country A will first have to comply with the data protection law of country A, and the data processing in country B will have to comply with the data protection law of country B. If B sends information to A, the situation changes. From the wording of art. 4(1)(a), the data protection law of country B will still be applicable to the case, even if the information now is in the hands of A. This rather complex situation could mean that A would have to separate all information according to where they come from, or comply with the strictest data protection law at the time. Inside a large community,[41] this means that one would at all times have to be looking at the possibility of new regulations and change internal routines.

But this problem has also another aspect: that is, a positive conflict of jurisdiction might arise. According to Bing:

> "The national data protection law of country B may, due to the close co-operation with the processing taking place at the main office, give its law extraterritorial application to the operation in country A. The result will have to be that the controller has to comply with the legislation of both country A and country B. As the law of both countries are harmonised by the Directive, this probably will not be too difficult, but due to the leeway of national choice in the implementation, one may have provisions which are in conflict in such a way that they cannot simultaneously be fulfilled – in this case the controller is in trouble."

---

40 Cf. Sect 2.8

41 Now counting 18 countries, and we do not include the two non-EU EEA-countries.

We do not pursue this question any further, but the controller must be aware of the difficulties concerning implementation of the Directive.

Until now we have taken for granted that there is only one controller and that this controller has one or several sub-branches situated in different countries. But, as noted above, art. 2(d) of the Directive seems to presume that there may be more than one controller per data-processing operation. In cases where this occurs, we may again be faced with a situation in which one set of data or one data-processing operation is subject to different national laws. This will not be a problem if the laws are in harmony – which is the assumption of the Directive – but such harmony might not eventuate given that states are given a significant "margin of appreciation" in implementing the Directive.

Problem 2: Can data mining be considered a contract between the data subject[42] and the controller? Can the contract derogate from the provisions of the Directive?

To the first question, it is quite clear that even a small web-wrap clause will be difficult to view as a contract. However, if the controller collects this information by, for example, a customer filling out a purchase, order or subscription form on the Internet, and the controller sends the customer a password to permit entry to the rest of the web-site, it is at least arguable that a contract has been made that is binding for the customer. It would be too speculative to attempt to draw any firm conclusions on this point, but it is probable that Continental-European conceptualisations of what constitutes a contract will be more restrictive than Anglo-American conceptualisations.

As for the second question, the Directive makes clear that one of its basic purposes is to protect human rights, in particular the right to privacy. This follows from art. 1(1):

> 'In accordance with this Directive, Member States, shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data ...'

It also follows from recitals 3, 7, 8 and 9 in the Directive's preamble. Accordingly, it could be argued that the Directive intends to set a "bottom-line" for protection of individual persons' fundamental rights. Thus, any contract which attempts to derogate from this bottom-line will probably not be tolerated, unless the controller "adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals ..." (Art. 26(2)).

Problem 3: Can the rules of* ordre public *stop data mining?

It is possible to envisage a situation where the court has given the parties jurisdiction and made a choice of law that is not the law of the jurisdiction in which the court is established; i.e., *lex fori*. If the law chosen offers a level of data protection far below that offered by the jurisdiction in which the court is established, there is a possibility that the court will refrain from applying the chosen law by reference to *ordre public* considerations. This possibility will increase the more the personal data concerned are sensitive and in need of stringent protection.

---

42 The data subject is the person to whom data relate; cf. art. 2(a) of the Directive.

4.2. Advertising and choice of law

It is suggested above that the execution of advertisement legislation is part of public law. It is an acknowledged principle that a national court as a point of departure never shall apply foreign law when judging cases of public matters. The general rule therefore is that when it comes to public law, the jurisdiction is not governed by the ordinary collision norms of private international law, whereas it is left for each of the country's practical possibilities to apply their own legislation and determine which law is applicable. Typically possibilities of applying national law will exist if the court has been found competent to adjudicate, see above.

Exceptions from the general rule will principally only take place in cases where international agreements form a different solution, and the state of the court is a party to the agreement. The question therefore becomes whether there are international agreements in Europe which regulate the questions of choice of law concerning advertisement on the Internet.

For the time being, no such agreement exists which regulates the problem directly. However there are two EC-Directives and one European Council Convention[43] concerning the questions of choice of law that concerns cross-border *broadcasting*. Advertising is one of the issues included.

The Directives and the Convention contain the principle that the lawfulness of a broadcast shall be assessed in accordance with the national legislation laid down in the country from where the broadcast originates, which in most cases will imply the country where the seat of the broadcasting company is situated. Given that the broadcasted commercial is in accordance with the advertisement legislation in the country from where the broadcast originates, one will normally not be allowed to restrain the retransmission of the broadcast in neighbouring countries, under the conditions that the contents of the broadcast violate their national rules.

> At least what concerns The Broadcasting Directive, this is not more than a starting point, see the decisions of the EC-court C-35/95 and C-36/95. In these cases it is, under certain circumstances, opened for the application of national law in situations like the one mentioned above. This is mostly due to the fact that the main purpose of the Directive is to oblige the parties not to restrict the retransmission of broadcast originating from other member states, whereas it does not necessarily address the right of the inhabitants to pursue their civil rights. Thus, one might say that even if the principle of "the country of origin" were to be applied to advertisement on the Internet, one could not be assured that the principle would apply under every circumstance.

The question becomes whether the principle of the choice of law laid down in the three mentioned instruments also should apply on advertisement on the Internet. One might adduce good reasons for that this should be the case. To apply the principle of "the country of origin" will simplify determining with which law the retailers will comply. This is because they will only have to consider the advertisement legislation of one country, instead of having to deal with the legislation in practically every jurisdiction of the world. Principles of equality may

---

43 "The Satellite and Cable Directive": Council Directive 3.10.1989 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities (89/552/EEC OJ 17.10.1989 298:25), "The Broadcasting Directive": Council directive of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities (89/552/EEC OJ 17.10.1989 298:25) as amended by the European Parliament and Council Directive 97/36/EC of 30.6.1997, and the European Convention on Transfrontier Television.

also be adduced for the support of applying the principle, as it might be inconsistent to let the choice of media in which the commercial is distributed determine the lawfulness of the content. The fact that cable television network may allow connection to the Internet by so called "cable modems", and that the differences from the Internet therefore becomes more subtle, also favours use of the same principles for the Internet as for advertising transmitted through the cable net. The EC Commission addresses this problem of convergence in their Green Paper on *Copyright and Related Rights in the Information Society.*[44] In the conclusion it is stated:

> "This would suggest that the applicable law ought to be the law of the Member State from which the service originates. But if that were to be made the rule, the laws of the Member States first have to be aligned very closely in order to avoid deflections of trade and loss of protection for right holders. The country-of-origin rule, which would take account of the different relays which might intervene in the transmission chain, could then be introduced once harmonization had been achieved. It remains to be seen whether this model can be applied to the exploitation of rights by the supplier of the service. This is the approach taken in the Satellite and Cable Directive."

Even if good reasons for why the principle of "the country of origin" should apply to advertisement on the Internet, it is still doubtful whether this is what the courts will choose in an actual case. This already follows from the general principle, which states that a court always shall apply its own national law in matters concerning public law. It is presumed here that there will have to be strong reasons to deviate from this principle. Provisions that are formed for the purpose of regulating television broadcasts cannot necessarily be assumed to have taken into consideration the necessary arguments to provide good solutions when applied on other types of media. One must also bear in mind the differences, which exist according to how the transmission of the advertisement takes place in the different types of media. While the broadcasting of a commercial inevitably will have to be considered an active action, it is not that obvious to argue the same when advertising on the Internet.

An additional remark is that the high costs involved with marketing products through television commercials will prevent the smallest and often less serious companies to utilise this medium for the advertisement of their products. It is likely that serious organisations to a greater extent will have an incentive to operate within the limits of normal decency. It may therefore be assumed that legal disputes concerning the contents of a commercial will not occur with the same frequency for television commercials as for advertising on the Internet, where the smaller cost implies that also less serious retailers will be able to market their products or services.

A final remark is that the *forum* country will be inclined to apply their own national law to adjudicate the legal disputes (*the homeward trend*).

Consequently, it is doubtful whether the Directives and the Convention will be applied by the courts, in the sense that the principle of "the country of origin" will apply also on advertisement on the Internet. Most likely, the courts will follow the general principle as mentioned above and apply their own national law.[45]

---

[44] Brussels 19.7.1995 COM(95) 382 final.

[45] However, the application of national law will require that the provisions are applicable on advertising on the Internet. This will in some cases be doubtful, see above.

4.3. Liability on the basis of loss suffered due to misleading information

4.3.1. Introduction

Liability may be both criminal and civil, and both forms could be the result of loss suffered due to misleading information. This report will not discuss criminal liability.

Misleading information is in many ways just a part of advertising and can occur through the advertising on the Internet, i.e. the information on the websites of Versand or Sainsbury's.

What kind of misleading information is this? First of all we consider this to be a prolongation of the commercial transaction. This implies that the misleading information has lead to an economical loss by the customers of Versand or Sainsbury's. Third party-situations are not discussed in this report.[46]

The kind of loss due to misleading information is primarily caused by the merchandise or product delivered by Versand or Sainsbury's. In the context of this report we will not discuss the liability questions solved by a potential contract. It must be mentioned, however, that if there were a contract[47] between the seller (Versand or Sainsbury's) and a customer, there would be certain limitations for what can be regulated on this contract. For consumer purchases notably, mandatory rules are guaranteed by the Rome Convention art. 5(2).[48]

Finally this would mean that the loss a customer may suffer due to misleading information, is the type which is not regulated in a contract. It can be the information the customer has trusted when purchasing the goods. When the customer then uses this product and it is not usable as predicted, the consumer might suffer a loss. The consumer might then have to purchase another product or borrow a product while the original product is being repaired. It may also be information misleading the customer not to take advantage of a favourable offer.

In the following we will pursue the choice of law that governs the liability, but first we will look at the regulation, or the lack thereof.

4.3.2. Regulations and the lack of these

Inside Europe the EU has issued several Council Directives dealing with misleading information and other problems like protection of consumers' interest. This field has been covered by Anne SALAUN in the Deliverable 13.

This is notably the Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising. This Directive gives a definition of misleading information in art.2(2):

> '...means any advertising which in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect their economic behaviour or which for those reasons, injures or is likely to injure a competitor ...'

---

46 Typical situations where Internet-surfers find information on the Internet and act on behalf of this, without doing anything more than looking at the web-site. Another third party is the one who's loss is based on wrongful information about him on this web-site, i.e. «Mr. A sells products fare worse than ours».

47 The Rome Convention states that the parties have full autonomy to make a choice of law, cf. art 2. This could again raise the question whether there is a binding contract between the parties, if this contract is due to a web wrap. We do not pursuit this question.

48 For a more extensive discussion, cf J. Benno: *Consumer purchases through telecommunications in Europe,* Complex 4/93 Tano (Oslo 1993).

This would mean that the misleading information we are discussing under this point of the report is similar to the term ''misleading advertising'' in the Directive. Unfortunately this Directive does not give any guidance as to what the choice of law should be in the context of loss suffered due to this type of advertising, even though it sets a standard for what the bottom line of misleading information cannot be.

Furthermore, there are Directives, which deal with the protection of consumers. Here we can mention the Council Directive 92/28/EEC on the advertising of medical products for human use, the Council Directive 93/13/EEC on unfair terms in consumer contracts, and even the Directive 97/7/EC of the European Parliament and of the Council on the protection of consumers in respect of distance contracts. Again, these Directives only set a certain standard for consumers, and they do not give a choice of law as to the liability when breaking these rules.

In the Directive 98/27/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interests, it is stated in art. 2(2) that:

> '... This Directive shall be without prejudice to the rules of private international law, with respect to the applicable law, thus leading normally to the application of either the law of the Member State where the infringement originated or the law of the Member State where the infringement has its effect ...'

As to what an infringement shall mean, this is stated in art. 1(2) dealing with the scope of this Directive:

> '...For the purpose of this Directive, an infringement shall mean any act contrary to the Directives listed in the Annex as transposed into the internal legal order of the Member States which harms the collective interests referred to in paragraph 1 ...'

The Directives of the Annex include the Directives listed above.

From this point there are several conclusions that can be made. The first conclusion is that in spite of the harmonisation inside the EU/EEA-system, the field of private international law still has a place. All cases addressing infringements in a private context, must first be solved through a private international law argument. The second conclusion suggests that the choice of law rule applicable to which law governs the liability question, is either the law of the Member State where the loss was originated or the law of the Member State where the infringement has its effect.[49]

As for the Directives mentioned above now, the conclusion must be that they might imply the application of a certain rule or rules, but these rules are not clear enough to suggest a choice of law for loss suffered due to misleading information. The only clear conclusion, from the Directive on injunctions for the protection of consumers' interests, must therefore be that private international law governs cases where there has to be a choice between several laws of the EU/EEA-community. This again brings us to the basic rules of private international law of liability outside of contract.

---

[49] It could though be argued that the choice of law process should go through two steps, one choosing the law to govern if there has occurred a loss(like if it where an infringement), and the second choosing the law to govern the liability. We believe that this is pointless, because both points still would have the same choice of law-rule.

4.3.3. The basic rule of private international law of liability outside of contract: lex loci delicti

As we saw in sect 2.7, there are several solutions to an international dispute. Everything from the domicile of the buyer or seller, to the use of *lex fori* is available. In contrast to this are the solutions concerning liability and infringements outside of contract. In private international law the basic solution for liability outside contractual obligations is the rule of *lex loci delicti*[50] – the law of the place of damage. This is normally quite clear in the field of physical damage, and the damage will mainly be located at only one place. For example two buses collide in country A. The busses do not come from this country, nor do they come from the same country. The law to govern the liability suit is the law of the country where the damage happened, i.e. country A.

The question is therefore whether the rule of *lex loci delicti* is applicable to solve liability due to misleading information in the context of a commercial transaction on the Internet. Looking at the problem there are two potential solutions: The law of the country where the damage has its origin, or the law of the country where the damage has occurred. These solutions have been outlined by the Directive 98/27/EC on injunctions for the protection of consumers' interests' art. 2(2). For a problem of loss due to misleading information, either the law of the country of the web-site[51] or the law of the country where the loss is suffered would apply. Both these solutions can have different outcomes.

The law of the web-site could be a solution, considering that the loss is due to the misleading information on the homepage. This homepage is then the natural source of the loss. Unfortunately it would be too easy for the web-owner to locate the server in a country with non-existing liability rules. In other words, the law of the web-site, as a simple rule, could lead to forum shopping.[52] Therefore the nearest solution is to apply the law of the web-site as the law of the country where the establishment operating the web-site is located. Not only would this follow the Directive 95/46/EC on Data Protection, but this would also correspond more with the intentions of the traditional rule of *lex loci delicti*. There are strong arguments for such a solution, mainly the predictability for all the parties. For the customer suing, this would also mean that his opponent has stable location. For the seller ('opponent') this implies the advantage of being always sued according to one set of rules. On the contrary this can also lead to an unfair situation; since the seller has accepted to sell on the Internet and thereby to a variety of countries, the liability should follow the place where the damage or loss is suffered.

Choosing the law of the country where the loss is suffered, is not as clear as it might seem, although the loss is clearly related to the person[53] that has purchased from the web-site in question. Unfortunately the ''loss'' can be related to several places. The places in question could be the domicile of the person that has suffered the loss, the place where the loss actually took place[54] or it could be the one the person's citizenship. Choosing the place where the loss actually took place, could here also mean the place where the economic loss took place or where the damage that caused the loss took place. Without going any further in this

---

50 See Helge J. Thue: *Norsk International obligasjonsrett, erstatning utenfor kontraktsforhold* (1986) UiO, Stensilserie nr.111.

51 The location of the web-site would here, in its simplicity, mean where the server that contains the web-site is situated.

52 Forum shopping refers to the situation where the party or the parties search for the law of a country that suits them best, and thereby they escape the natural court.

53 Could be legal or physical.

54 Which is not the one of the domicile or citizenship.

discussion, and without trying to solve a problem any court has decided, we would suggest the law of the country of the domicile of the person that has suffered the loss.

Trying to determine whether the *lex loci delicti*-rule of private international law is applicable to the problem raised by loss due to misleading information, causes many difficulties, mainly because this cannot be anything more than an assumption. On the other hand the rule of *lex loci delicti* is still a part of private international law. The best solution to this rule would, in our opinion, then be to make the choice of law according to the country of the establishment behind the web-site.

Unfortunately the rule of *lex loci delicti* is not the only candidate. The simple choice of law rule based on the geographical relation seems to have certain insufficiency. Some courts would seem in favour of applying *lex fori*. Inside the EU/EEA, where the Lugano and Brussels Conventions determines the jurisdiction,[55] and where the geographical relation between the loss and the jurisdiction has placed the lawsuit in one court, it is not unlikely that the court will apply *lex fori*. This would follow the unfortunate ''homeward trend''. However the latter solution is not acceptable in the context of private international law.

Finally another suggested solution to these problems is, the so-called 'principle of closest connection'. The closest connection is found by considering all circumstances of the transaction which may serve as connecting elements, weighing them together and then determining where the contract has its natural centre of gravity,[56] i.e. the closest connection. The connecting elements will then be all the elements mentioned above; from the place of the web-site, the establishment behind the web-site, the country of the buyer, the language of the web-site to elements like where the loss was suffered. This method has a certain flexibility, which is lacking in the other solutions. On the other hand, this method has a large portion of unpredictability. This is why the method has not been fully accepted. Finally it must be said that this solution has been adopted by the 1980 Rome Convention on the law applicable to contractual obligations, cf. art 4(1) on applicable law in absence of choice:

> ''To the extent that the law applicable to the contract has not been chosen in accordance with Article 3, the contract shall be governed by the law of the country with which it is most closely connected...''

If a contract between two parties does not have a choice of law-clause, the solution is the method of the closest connection. This method has also been adopted by the courts, but one could argue that they apply this in cases where the basic rule of private international law does not correspond with their ideas. However there is one leading Norwegian case to illustrate this method. Bing has written in relationship to this matter:

> ''In Norwegian law, there is a famous case of two Norwegian ships colliding in the Mouth of Tyne, and where there was a difference between the maritime law of England and Norway with respect to the liability. Here there was no doubt that the 'injury' took place in British territory, but Norwegian courts found that there under the circumstances were no reasonable justification to decide a case between two Norwegian ship owner according to foreign law [whereafter they applied Norwegian law]. The names of the two ships were Irma and Mignon, and the Principe of the closest connection has in Norwegian theory survived as the Irma-Mignon formula''[57].

---

55 See Sect 3.2.

56 Term first used by C.F. Savigny.

57 Rt. 1923 s. 59

We have explored the different solutions to the question of what rules could be applied to make a choice of law as to liability. As to drawing a conclusion we find this to be a matter for the reader, and not for us. Though we suggest that the solution should be the one that gives both parties in a lawsuit certain predictability.

4.3.4. The limitations of the choice of law

As already stated in previous parts of this report, the choice of law might conflict with the *ordre public* of the court. It is quite possible that the large amounts of compensation damages given in the USA, will not be given in a European court if the choice of law happens to be American law. In a lower Norwegian court[58] in 1985 there was a liability law-suit against a Norwegian. The choice of law was the Austrian law. On the basis of some sort of *ordre public* argument, the court decided to use the Norwegian limitation rule of 3 years for determining whether damages could be claimed, and not the Austrian limitation rule of 30 years.

5. CONCLUSION

Concluding with respect to issues where the uncertainties are as great as in private international law, can only be speculations. Trying to give clear answers might lead to further problems. Even so, we will try to give a short summary of this report as a sort of conclusion.

Considering the jurisdiction in Europe, the Lugano and Brussels Conventions will solve the problems of jurisdiction for private and commercial matters. For the parties addressing a court, these conventions give security as to always finding a jurisdiction. As for where this jurisdiction will be, there might be problems. And if it does, the European Court of Justice may be able to give a prejudicial judgement. Further problems arise in the field outside private law. In such cases, like advertising, public law causes problems in the digital world, mainly because they imply national jurisdiction. The location of an Internet web-site offering advertisement is not as certain as the location of the person accessing the web-site or the provider of the web-site. Any further conclusions can not be expected.

As for choice of law, there are different solutions for different issues. Unfortunately there are not too many international regulations available.

The choice of law in data protection, is easy to solve for a simple case, but as quickly more controllers enter the stage, the problems abound.

For advertising, the choice of law is not governed by any regulations and the only solutions would be to apply analogue regulations. If this is acceptable is not easy to say.

The choice of law in the context of liability for loss suffered due to misleading information, the traditional rule of *lex loci delicti* must be said to compete with the method of the closest connection. This is how far we can dare to suggest a solution.

Finally this leads us to conclude that the digital world can not be said to be completely compatible with analogue world. The traditional solutions given in the existing Directives or conventions, like the Brussels Convention, are not directly applicable to the digital world. The first cases dealing with these questions will therefore be very decisive. The EU may have to adopt new regulations directly applicable to the digital world. The latter solution would be welcome, implying a harmonisation of private international law in this field and offer increased predictability for the parties.

---

[58] Appelate Court Decision (Eidsivating lagmannsrett, RG 1985 s 778).

ANNEX 4 : Assistance to TRADE : legal issues of the pilot applications and of the TRADE server

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

ASSISTANCE TO TRADE : Identifying the Legal Issues

Authors : CRID, ITM, QMW, UIB, NRCCL

11 December 1998

CONTENTS :

Authors : CRID (Sophie Louveaux, Rosa JULIA BARCELO, Séverine DUSOLLIER), ITM (Volker KABISCH,

Matthias BUENING), QMC (Laura Edgar), UIB (Jose Lluis MATEO HERNANDEZ), NRCCL (Peter LENDA, Morten FOSS)

I. INTRODUCTION

The TRADE project is strongly oriented to develop pilot applications whose purpose is to test the E-Commerce Reference Model and the TRADE application server. Based on these pilots trials, the customer's satisfaction will help validate the adopted technical solutions. In addition to user's acceptance (buyer, seller and business intermediaries) and costs and benefits of the TRADE approach, the legal constraints should be integrated as well in the design and development of the TRADE Model.

Therefore, this first assistance paper from ECLIP encompasses both the legal aspects raised by the TRADE server and by the pilot application, wich represents the first two tasks to be carried out for TRADE project.

The first part considers the legal issues raised by the operation of the TRADE server in itself.

The second part is limited to an overall consideration of the legal issues arising in the pilot applications developed in the project TRADE. Two Pilot applications have been reviewed by E-CLIP partners on the basis of the deliverable 5 and 7: on one hand the so-called "ticketing scenario" which sets up an on-line broker systems for reservation and provision of tickets for cultural and sports events, on the other hand the so-called "administrative and legal scenario" which sets up a service for providing administrative and legal services on-line.

This paper raises legal issues to be considered by TRADE partners when designing and launching both the TRADE server and each application. We have particularly considered those legal issues that are specific to e-commerce scenario.

II. LEGAL ISSUES OF PILOT APPLICATIONS

1. DIGITAL SIGNATURE

1.1. INTRODUCTION.

Open networks such as the Internet are of the increasing importance for world-wide communication. They offer the possibility of interactive communication between parties who may not have pre-established relationships. They offer new business opportunities by creating tools to strengthen productivity and reduce costs, as well as new methods of reaching customers.

In order to make best use of these opportunities, a secure environment with respect to electronic authentication is needed. Several different methods exist to sign documents electronically varying from very simple methods (e.g. inserting a scanned image of a hand-written signature in a word processing document) to very advanced methods (e.g. digital signatures using "public key cryptography").

Electronic signatures allow the recipient of electronically send data to verify the origin of the data (*authentication* of data source) and to check that the data are complete and unchanged and thereby safeguard their integrity (*integrity* of data).[1]

The digital signature is an essential tool for providing security and developing trust on open networks and we must know its real meaning as a key issue for electronic commerce. The TRADE PROJECT needs this tool because some of the information should be confidential and others don't need confidential but must preserve integrity.

1.2. SECURITY IN E-COMMERCE.

Internet is a global, but insecure, network and Cryptography can contribute greatly to the transactional security that Internet commerce lacks.

Cryptography must solve four basic questions about security in electronic commerce:

1. **CONFIDENTIALITY** of the data transaction.
2. **INTEGRITY**: protection against data modification.
3. **AUTHENTICATION** of the different partners and other entities involved.
4. **NON REPUDIATION**: no entity should be able to deny that he has sent a message.

These objectives are important for merchants and buyers. The next problem is that implementing and using a digital signature and a Certification Authority, we can't prove the reception of the message (NON REPUDIATION IN RECEPTION). This objective is only possible by means of an acknowledgement of receipt or the intervention of a third party.

Before embarking on a discussion of the role and structure of digital signatures, it is useful to review basic cryptography techniques as private and public- key cryptography.

a) **Private-key cryptography**: There is only one key. The seller and the buyer know it and *the problem is the insecure transmission of the key*.

[1] "*Proposal for a European Parliament and Council Directive on a common framework for electronic signatures*". Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions.

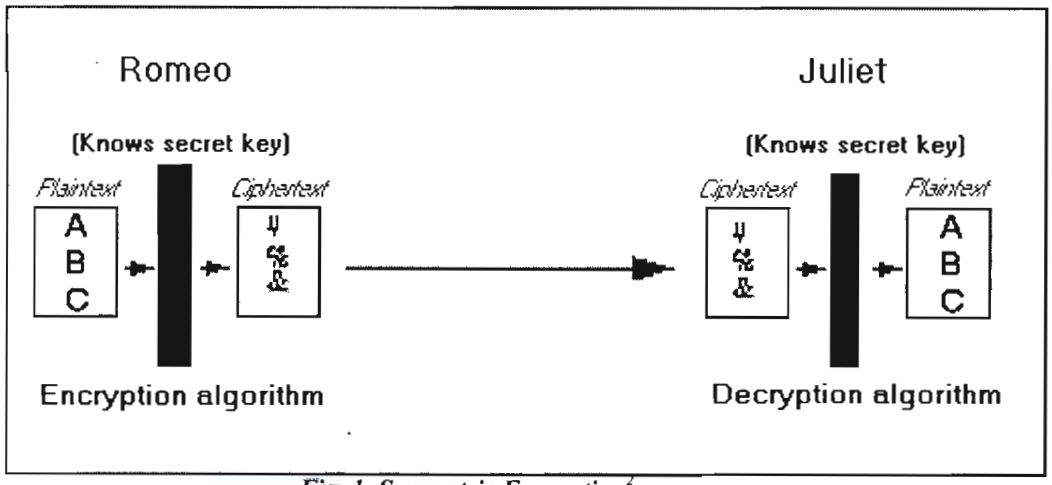


Fig. 1 Symmetric Encryption[2]

It's necessary to use the same key to encrypt and decrypt the message, and this system has the positive point that it's faster than the other one we are going to explain (e.g. the **DES** system).

Fig. 2 Symmetric Encryption[3]

b) **Public-key cryptography**: The messages encrypted with one key can only be decrypted with a second key, and vice-versa. The system gets its name from the idea that the user will publish one key, but keep the other secret. The world can use the public key to send messages that only the private key owner can read; on the other hand, the private key can be used to send messages that could only have been sent by the key owner (e.g. the **RSA** system).

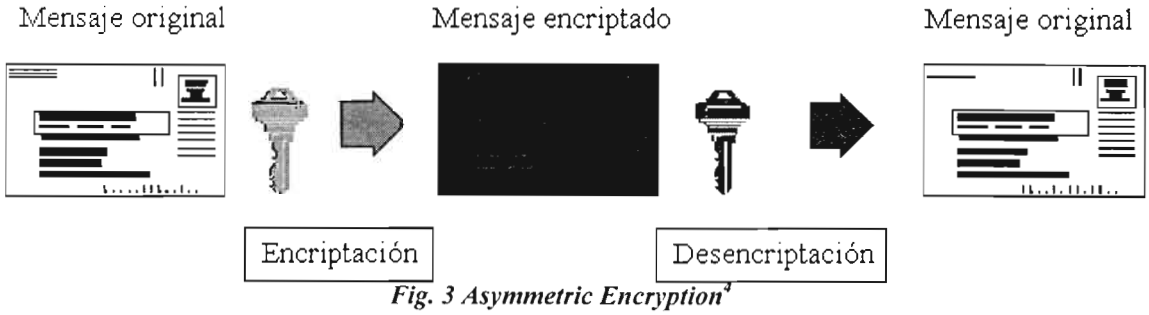
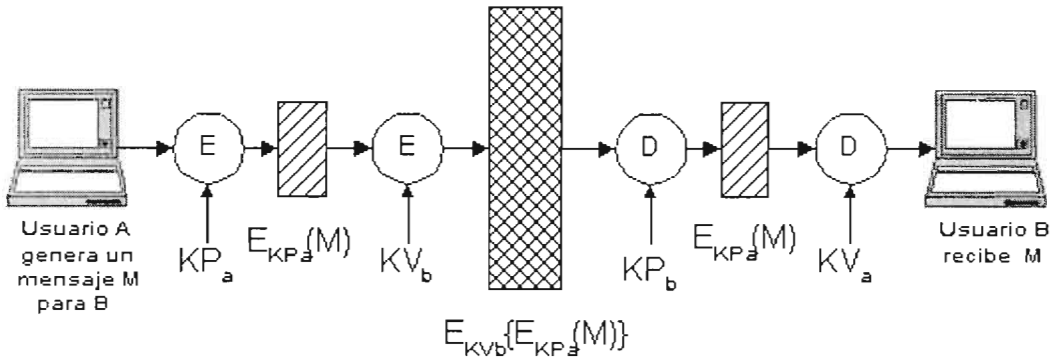


Fig. 3 Asymmetric Encryption[4]

[2] Design imported from www.ispo.cec.beeif/policy/97503annex.html.
[3] Design imported from www.kriptopolis.com.
[4] Design imported from www.kriptopolis.com.

If A encrypts the message with the public key of B (recipient), then only B will decrypt it (confidentiality). If A encrypts with his private key, anybody can decrypt the message with A's public key, but authenticity and non repudiation are guaranteed. And if A encrypt the message mixing both systems, then the question is solved.



The problem is that an asymmetric and direct encryption of the message means a very slow process. That is the reason we have to talk about digital signatures (they are the solution of this problem).

1.3. DEFINITIONS AND FUNCTIONS.

First of all, legislation that has been enacted or proposed addresses two different categories of signatures, electronic and digital signatures. The more general term ***"electronic signatures"*** is generally defined as any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with an intent to authenticate a writing. A ***"digital signature"***, on the other hand, is a subset of electronic signatures that is defined by the use of asymmetric cryptography to create the mark used to manifest intent by the signer. In the U.S.A., for example, the different legislation in each state addresses either electronic signatures (23 states) or digital signatures (15 states), but not both. The only exception is the proposed Illinois legislation.

We must study digital signatures and we can find a great number of definitions that show us its relevance[5], but the most relevant concept is content in the *Proposal for a European and Council Directive on a common framework for electronic signatures:*

[5] State of Arizona (U.S.A.): "A type of electronic signature that transforms a message through the use of an asymmetric cryptosystem."
State of Florida (U.S.A.): " Digital signature' means a type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: a) Whether the transformation was created using the private key that corresponds to the signer's public key; b) Whether the initial message has been altered since the transformation was made."
State of Illinois (U.S.A.): " Digital signature means a type of an electronic signature created by transforming an electronic record using a message digest function, and encrypting the resulting transformation with an asymmetric cryptosystem using the signer's private key such that any person having the initial untransformed electronic record, the encrypted and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key; and whether the initial electronic record has been altered since the transformation was made. A digital signature is a security

Article 2: For the purpose of this Directive:

1.Electronic signature means a signature in digital form in, or attached to, or logically associated with, data which is used by a signatory to indicate his approval of the content of that data and meets the following requirements:

a) It is uniquely linked to the signatory,

b) It is capable of identifying the signatory,

c) It is created using means that the signatory can maintain under his sole control, and

d) *It is linked to the data to which it relates in such a manner that any subsequent alteration of the data is revealed (...)*

Digital signatures solve the authentication, integrity and non-repudiation from sender problems. Transforming an electronic record using a message digest function creates a digital signature. This is the first step: using the HASH algorithm[6] we can get the digest of the message.

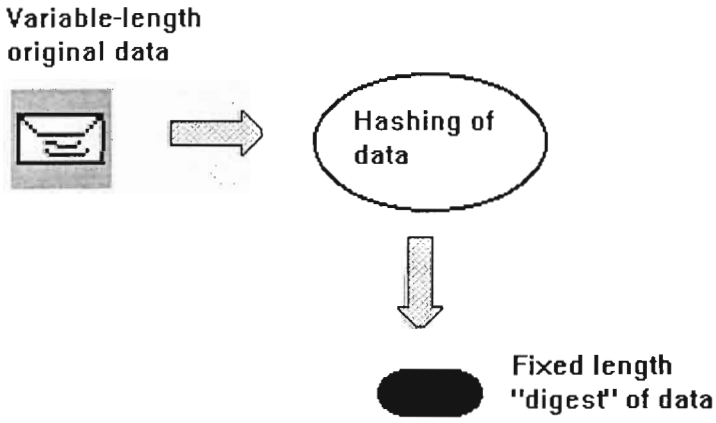
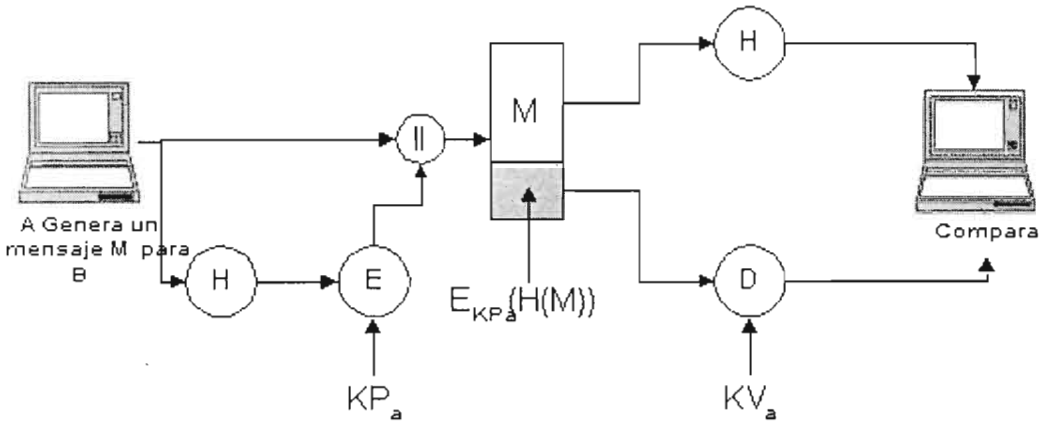


Fig. 4 Digital Signature[7]

Then it's necessary to encrypt the digest using A's private key and send it with the original message. The recipient will calculate the digest of the original message and will compare it with the first digest. Authenticity (using A's private key), and integrity (digest) are guaranteed.

procedure."

[6] An unidirectional system to get a digest of the message.
[7] Design imported from www.ispo.cec.be/eif/policy/97503annex.html.



On the other hand, we need confidentiality and one of the correct ways to get that objective is using the digital envelope by combining symmetric and asymmetric system.

We have to encrypt the message with the symmetric system (DES key), and the symmetric key will be encrypted with the public key of the recipient. Then the recipient will decrypt the symmetric key with his private asymmetric key to finally decrypt the message. E.g. the RSA digital envelop.

We finally have to talk about the Certification Authorities. If A and B are strangers with no alternate means of communication then no digital signatures, indeed no amount of cryptography standing alone, will reliably authenticate or identify them to each other without the assistance of some outside source to provide a link between their identities and their public keys. Any outside source that reasonably inspires trust will suffice. A Certification Authority (CA) is a body, either public or private, that seeks to fill the need for trusted third party services in electronic commerce by issuing digital certificates that attest to some fact about the subject of the certificate.

In order to either A or B to be willing to accept certificates issued by C (a CA), A and B must have confidence that C's public key is really C's and not another wrong manifestation. One way to achieve this confidence is to have an identifying certificate from D (another CA), certifying C'S key. Cas that certify other Cas are said to participate in a *certificate chain*, with a *root certificate*, at the bottom of the tree.

A certificate is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person proffering a digital signature. More formally, a certificate is a computer-based record which: a) identifies the CA issuing it, b) names, identities, or describes an attribute of the subscriber, c) contains the subscriber's public key, and d) is digitally signed by the CA issuing it. In practice, Cas will probably offer a range of certificates, graded according to the level of inquiry used to confirm the identity of the subject of the certificate.

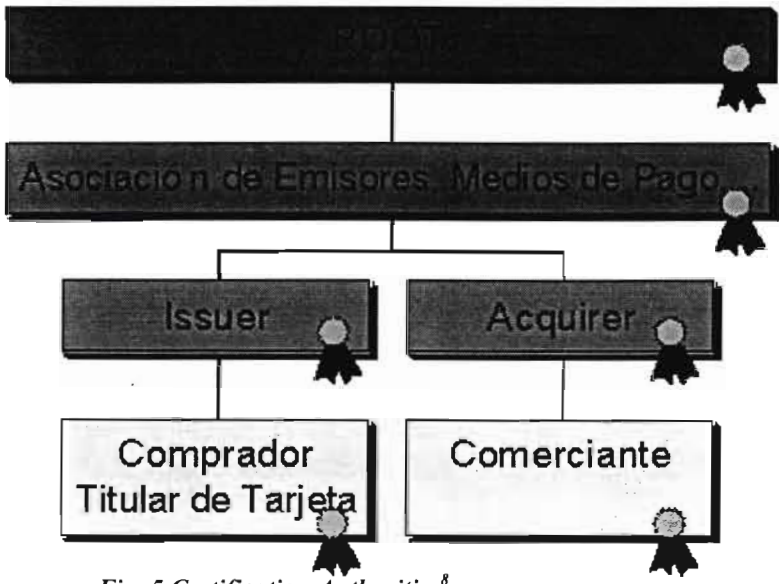


Fig. 5 Certification Authorities[8]

1.4. ENACTED LEGISLATION.

We can find enacted legislation about digital signatures in the U.S.A. and in Europe (Utah was pioneer in this aspect). Now, most of the States (U.S), have their own regulation but in general the different specialists, lawyers, doctors and Professors think about the need of an uniform and global regulation. The last steps are the ***Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions*** with a *Proposal for a European Parliament and Council Directive*, (that talks about the increasing legislative activity in this area in several Member States[9] and the need for a harmonised legal framework at the European level so as to avoid, the development of serious obstacles to the functioning of the Internal Market), and the ***United States Proposal for "Draft International Convention on electronic Transactions"*** (it establish general obligations that show the global thinking of the International Community: modification of existing rules and minimal adoption of new rules, party autonomy, all authentication technologies and business methods may be evidence of authenticity, technology neutrality, implementation neutrality, non-discrimination and avoid unnecessary barriers to trade).

We also talk about the ***UNCITRAL Model Law on Electronic Commerce (1.996).*** *"The Article 7 of this Model Law is based on the recognition of the functions of a signature in paper-based environment In the preparation of the Model Law, the following functions of a signature were considered; to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; to associate that person with the content of a document. It was noted that, in addition, a signature could perform a variety of functions, depending on the nature of the document that was signed..."*

[8] Design imported from www.kriptopolis.com.
[9] Germany, Italy and the U.K. have Digital Signature Legislation enacted in Europe. This information is available in Internet (http://www.mbc.com)

But the most interesting legal text is the ***Proposal for a Directive establishing a legal framework for the use of electronic signatures.***[10] The main elements of the proposed Directive are the following:

- **Essential requirements**: the proposal would define essential requirements for electronic signature certificates and certification services so as to ensure minimum levels of security and allow their free movement throughout the Single Market. These requirements would include personal reliability, use of trustworthy systems and a ban of storing private signature keys.

- **Liability**: the proposal would establish minimum liability rules for service providers, who would in particular be liable for the validity of a certificate's content. This approach will ensure the free movement of certificates and certification services within the Single Market, build consumer trust and stimulate operators to develop secure systems and signatures without restrictive and inflexible regulation.

- **Legal recognition**: the proposal would stipulate that an electronic signature could not be legally discriminated against solely on the grounds that it is in electronic form, as the legal effects of electronic signatures are essential for an open system. If a certificate and the service provider met certain essential requirements, electronic signatures based en their service would benefit from an automatic assumption that they were legally recognised in the same manner as hand-written signatures.

- **A technology-neutral framework**: the proposal provides for legal recognition of electronic signatures irrespective of the technology used.

- **Scope**: the proposal concerns the supply of certificates to the public aimed at identifying the sender of an electronic message, but does not apply to closed user groups such as corporate Intranets or banking systems, where a trust relation already exists and where there is therefore no obvious need for regulation.

- **Certification**: certification services could be offered in principle without authorisation, in view of the fact that technology and the market are evolving rapidly and as market forces will encourage high levels of security to satisfy consumers' concerns. Member States would be free to set up voluntary accreditation schemes for certification service providers in order to indicate special security measures or levels.

- **International dimension**: in order to facilitate electronic commerce at world level, the proposal includes mechanisms for co-operation with third countries on mutual recognition of certificates on the basis of bilateral and multilateral agreements.[11]

1.5. CONCLUSIONS.

Taking as initial point **the *Proposal for a European Parliament and Council Directive on a common framework for electronic signatures***, we can deduce these important conclusions:

---

[10] It has been put forward on 13 May 1.998 by the European Commission, on the initiative of Telecommunications Commissioner Martin Bangemann and Single Market Commissioner Mario Monti. By laying down minimum rules concerning security and liability, the proposal would ensure electronic signatures were legally recognised throughout the EU on the basis of the Single Market principles of free movement of services and home country control.

[11] The proposed Directive comes as a follow up to the *Communication on Ensuring security and trust in electronic communication- Towards a European framework for digital signatures and encryption,* adopted by the Commission in October 1.997.

1. It's important to get a *web certificate* with trusty Certification Authorities to provide secure services in the tree trials you present.

2. If it were necessary to *authenticate the buyer* in the concrete selling process (e.g. it should be advisable in the case of the professional client in the first trial), it would be important to fix the requisites of each certificate that this buyer has to use (more or less secure certificates).

3. If a digitally signed document with its certificate must be presented in a legal process, the Judge conviction will depend on the *neutrality* of the Certification Authority regard to the parties. That is the case of the second project).

4. It's necessary to use the web's public key to encrypt the information sent by the consumer *(confidentiality)*, especially if personal data, numbers of account etceteras are included.

5. If the user wants to be sure of the celebration of the contract with the message he's sent, it's necessary to implement a formal *acknowledgement of receipt* or the specific action of a *trust third party.*

6. It's essential to *inform the consumer* about the complete procedure and the security guarantees.

7. It's possible to find some *specific legislation* with especial limitations or concrete requisites for using the digital signatures as equivalent of written signatures (e.g. all about legal proceedings). This is especially remarkable related to the second trial that implements some judicial communications.

2. INTELLECTUAL PROPERTY RIGHTS ISSUES

As regards Intellectual Property Law, the TRADE trials in which ECLIP will be involved give rise to very few questions. TRADE will have the usual copyright and trademark problems that concern everyone who puts a web site onto the Internet or another network. (see below I). Besides that, the multimedia catalogue of cultural events that is foreseen within the ticketing scenario leads to some specific copyright-related questions (see below II).

I. IPR aspects common to both trials

When establishing a web site for the ticketing and for the consulting trial, TRADE will probably make use of texts and pictures protected by copyright law or by neighbouring rights. Thus, the project will be interested in knowing which parts of the web content are protected. It will also ask if the web site as such is protected by copyright law. In case that ECLIP holds that TRADE makes use of copyrighted elements, TRADE will have to know who is the rightholder (employee of a TRADE partner or third party). The next question will concern the relevant exploitation right. Beneath a reproduction act carried out when storing the material on the TRADE server the actions will have to be deemed as public performance.

TRADE will not benefit from a statutory licence. Thus, the project might need assistance for drafting the necessary licensing agreements. This assistance could be carried out by proof-reading of the pre-existing contracts.

It is unlikely that TRADE will be interested in trademark law-related assistance. Questions would only arise if TRADE used a third party¥s names as domain or vice versa.

II. Specific problems of the ticketing scenario

Within the ticketing trial customers, both business and residential, will be enabled to check the availability of tickets, to book, to pay and to receive the ticket via the Internet or another network. It is not clear if the tickets TRADE disseminates over the Internet and by help of a printer in the ticket agencies will contain protected material, e.g. a picture of the artist. In this case it would be doubtful if, beneath the reproduction right, the distribution right or the public performance right is concerned.

The most interesting activity within the ticketing trial will be the multimedia catalogue of events, which will be used as a marketing instrument. The documents submitted by TRADE do not specify what this catalogue will look like. In case of music events it will probably contain samples of the artist's music, pictures and video clips from a concert or recital. In case of theatre tickets TRADE might offer pictures and clips from the play, in case of exhibitions the customer might find some reproductions from the pictures or sculptures shown in the exhibition. The catalogue might also try to capture the customer's interest by pictures and videos containing information about sports events.

For this catalogue, TRADE will need licences. Thus, it is again important to know if copyrights or neighbouring rights are concerned, who the rightholders are, which exploitation right is needed (reproduction and public performance).

III. Specific problems of the consulting scenario

Within the other trial in which ECLIP will be involved, i.e. the legal and administrative consulting scenario, IPR-related questions do not arise. In this trial there will be no on-line transmission of copyrighted material. In Spain and Italy as Civil Law countries legal documents and forms usually are not protected by copyright law. Thus, TRADE will need no licences.

An important legal aspect of the consulting scenario will be the legal constraints to advertising for lawyers and taxation consultants. These stipulations will have an important impact on the form and content of the web sites. But since the rules of professional conduct are not covered by ECLIP, this will be of no importance for the assistance.

3. DATA PROTECTION ISSUES

The protection of personal data in the European Union is afforded by national data protection laws who must transpose the EU directive 95/46/EC (General directive) on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Following are a few comments which arise when applying the general directive to TRADE trials applications.

I. PERSONAL DATA

The directive applies to the processing of personal data wholly or partly by automatic means. The first question which arise is therefore whether or not personal data is being processed within the context of the TRADE applications scenarios.

The entertainment scenario primarily concentrates on Business-to-Business and Business-to-Individual scenarios. The data in the entertainment application scenario concerns professional users (e.g. box office, tickets agencies) and event owners rather than data concerning the actual buyer of the tickets himself (private client). In the context of Business-to-Business scenarios data protection rules do not generally apply because we are not dealing with data relating to identified or identifiable individuals. However some national data protection laws (i.e. the Italian law on data protection) include data relating to legal persons in the scope of the protection afforded. If data regarding private clients is transmitted, then one is correct in saying that personal data relating to an physical person is being processed. One can underline that at the moment that no financial data is being processed.

In the legal scenario, if in principle the data concerns a legal service rather than a natural person, the information transmitted could concern the customer himself and therefore could be considered as personal data (the customer could be required to provide a document containing personal data regarding himself). The data could also involve a third party involved in a case with the customer, for example. In such a case the third party will need to be informed that personal data relating to him is being processed. The service could also involve financial data necessary for the payment of the service.

The administrative scenario does not in principle contain personal data, but like the legal scenario the customer could be required to submit personal data and likewise financial data is involved for the payment to the administration.

II. CONTROLLER

The data protection principles imply the existence of a "controller" who will be responsible for ensuring the respect of the data protection principles. The controller is defined in the directive as the "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the means and purposes of the processing of personal data".

It would seem from the outset that in the entertainment scenario, BEL must be designated as such a controller in the BEL scenario and in the entertainment scenario since it defines the means and the purposes of the systems.

In the legal/administrative scenarios one must examine who defines the means and the purposes of the system. This will vary according to the service offered.

The designation of the controller will also be important in that it will determine which national law will apply. Indeed according to the directive the law of the country where the controller is established will apply[12]. If the controller is established on the territory of several Member states each establishment must respect the obligations of the national laws applicable.

III. Data protection principles

According to article 6 of the directive, personal data must be processed fairly and lawfully. Fair processing implies a maximum of openness. Lawfulness implies that the data protection principles must be respected. The data must be processed for legitimate, specified and explicit purpose and must not be further processed in a way incompatible with that for which the data was initially collected. This implies that the controller must determine at the outcome what the data is being collected for, must inform the data subject of this purpose (see later right to be informed), and must not process the data for any purpose which is not in line with the purpose for which the data was initially collected

[12] According to the recitals ß19 of the directive, the establishement of a controller in a Member state implies "effective and real exercise of an activity through stable arrangements".

without informing the data subject. The processing of data for statistical purposes is not, according to the directive, considered as incompatible providing the Member states provide the adequate safeguards.

Article 7 lays down grounds on which the data processing must be based. In the context of the Trade applications, the processing could either be based on the data subject having given his unambiguous consent; if the processing is necessary for the performance of a contract to which the data subject is a party or in order to take the steps at the request of the data subject prior to the entering of the contract; or if the processing is necessary for compliance with a legal obligation to which the controller is subject (this could maybe be the case in the legal and administrative scenario).

As for data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life", it is in principles prohibited unless it can be based on grounds laid down in article 8.2. of the directive. Data relating to offences, criminal convictions may only be processed under the control of official authority or if specific safeguards are provided under national law. Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority. This could have implications for the processing of such data in TRADE legal scenarios.

Data quality implies that the data must be adequate, relevant and not excessive with regard to the purpose for which it was initially collected.

The data must be accurate and kept up to date. Every reasonable step must be taken to ensure that data, which are incomplete or inaccurate, are either erased or modified.

The data must not be kept in a form which permits identification of the subjects for longer than is necessary for the purposes for which the data were collected or for which they were further processed.

IV. Rights of the data subject

The data subject is granted with a number of rights. It is up to the data controller to ensure that these rights are respected.

The data subject must be informed of a certain number of items. If the data is collected directly from the data subject, article 10 provides that the data subject must be informed at least of the identity of the data controller and the purpose of the processing. He must be further informed of any information such as the recipients or categories of recipients, whether replies to questions are obligatory or not, as well as the consequences of the failure to reply if such information is necessary to guarantee fair processing in respect of the data subject.

If the data is not directly collected from the data subject, the data subject must be informed either when the data is first recorded or when the data is first communicated. Information covers the same data as that mentioned in article 10 plus the categories of data concerned if necessary to ensure fair processing.

Article 11.2 does however provide for an exemption to the duty to inform for statistical purposes if the provision of such information proves impossible or would involve a disproportionate effort.

The data subject also has the right to have the confirmation of the existence of data about him being processed and information about the purposes of the processing, categories of data and categories of recipients. He may also receive the communication in an intelligible form of the data undergoing processing and of any available information about the sources of the data.

This right of access of the data subject to his data must be granted without constraint at reasonable intervals and without excessive delay or expense. If appropriate the data subject is granted with the right to the rectification, erasure or blocking of data in particular because the data is incomplete or inaccurate.

The data subject also has the right, on compelling and legitimate grounds, to object to the use of his data. This right is granted unconditionally as concerns data collected and used for direct marketing purposes (see article 14.b of the directive).

Finally, the data subject is granted with the right not to be subject to individual automated decisions that is to say decisions which produce a legal effect concerning him or which significantly affects him and which is based solely on automated processing of data intended to evaluate certain aspects relating to him such as his creditworthiness, reliability, conduct, etc...

V. Duties of the controller: Notification, security and confidentiality

The controller of the data must notify a national supervisory authority prior to the processing of the data.

The controller must also ensure that the appropriate technical and organisational measures are set up to protect personal data against accidental or unlawful destruction or loss of the data. These measures must be taken with regard to the risks represented by the processing and the nature of the data and must be taken with regard to the state of the art and the cost of their implementation. Persons processing data under the authority of the controller may only process the data if required to do so by law or under the instructions of the controller. The controller must lay down instructions to any person processing data on his behalf (processor) in a contract or legally binding act.

VI. Transborder data flows

Personal data may only be transferred to countries outside the European Union if this state offers an adequate level of protection according to the Member states and the European Commission. The Commission has developed a series of criteria in this respect in its article 29 Working Group. Any transfer of data must therefore be to a country which affords this protection unless the transfer can be based on an exemption found in article 26 of the directive an notably if the data subject has given his consent unambiguously to the proposed transfer or if the transfer is necessary for the performance of a contract between the data subject and the controller.

4. CONSUMER PROTECTION ISSUES

I. Consumer Protection issues common to both trials

a) Application of consumer protection regulations

Both trials are aimed at providing goods or services either to a consumer (called a 'private client in the entertainment scenario) or to business. When dealing with a consumer, a number of national and European regulation for protection of consumers' interests should be complied with, mainly the

Distance Contracts Directive 97/7/EC and the Council Directive 93/13/EC on unfair contract terms in consumer contracts.

In both Directives, the consumer is defined as " any natural person who is acting for purposes which are outside his trade, business or profession".

Distance contracts Directive

The Directive applies to _distance contract" which means any contract concerning goods and services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded[13].

The Directive applies only to contracts whose conclusion itself takes place at a distance.

The "means of distance communication" are defined as any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the conclusion of a contract between those parties[14].

Such techniques as videotext, e-mail, fax and television are notably targeted. Information Society Services and contracting via the Internet are not explicitly covered by the Directive but its definition of the 'means of distance communication' has been broadly construed to include such new technologies.

The operator of a means of communication is any public or private natural or legal person whose trade, business or profession involves making one or more means of distance communication available to suppliers. Therefore, compliance with the Directive principles should be considered when designing and setting up both pilot application, the entertainment scenario and the legal and administrative services.

This principles can be summarised as follows :

- Prior Information: In good time prior to the conclusion of any distance contract, the consumer must be provided with information[15] concerning :

(a) the identity of the supplier and, in cases requiring payment in advance, his address,

(b) the main characteristics of the goods and services;

(c) the price of the goods or services including taxes,

(d) delivery costs, where appropriate,

(e) the arrangements for payment, delivery or performance,

(f) the existence of a right of withdrawal,

(g) the cost of using the means of distance communication, where it is calculated other than the basic rate,

---

[13] Article 2 ß1 of the Directive

[14] Article 2 ß4 of the Directive

[15] Article 4.

(h) the period of time for which the offer remains valid,

(i) the minimum duration of the contract.. (Article 4 (1))

For contracts that are intended to be entered into on the Internet, it is ideal for this type of information to be included on a website in a clearly accessible manner.

- Written confirmation of information : Article 5 provides : "the consumer must receive written confirmation or confirmation in another durable medium available and accessible to him of the information referred to in Art. 4(1)(a) to (f), in good time during the performance of the contract, and at latest at the time of delivery ...

In any event the following must be provided :

- written information on the conditions and procedures for exercising the right of withdrawal,
- the geographical address of the place of business of the supplier to which the consumer may address any complaints,
- information on after-sales services and guarantees which exist,
- the conditions for cancelling the contract, where it is of unspecified duration or a duration exceeding one year. "

- Right of withdrawal: As a rule, for any distance contract, the consumer will benefit from a period of at least 7 working days in which to withdraw from the contract without penalty and without giving any reason. The supplier will then be obliged to reimburse the sums paid, free of charge[16]. However, an exception is provided, which will probably apply to the on line distribution of protected material: Unless the parties have agreed otherwise in respect of certain types of contracts, such as for the provision of services, if the performance has begun with the consumer's agreement, before the end of the seven working day period, for the supply of newspaper, periodicals and magazines or for the supply of audio or video recordings or computer software which were unsealed by the consumer.
- Performance: Again, unless the parties have agreed otherwise, the supplier must execute the order within a maximum of thirty days from the day on which the consumer has forwarded his order to the supplier[17].

[16] Article 6 1. and 6.2..

[17] Article 7 1.

II. Ticketing scenario

a) Commercial communications and advertisements

In the entertainment and tickets reservation scenario, it is said that the Information Broker is in charge of providing product information and marketing. Two sub-activities are particularly relevant here. On one hand, it is planned that the Information broker will accumulate and analyse customer patterns. This collection of data might raise important concerns from a privacy and data protection point of view (see part on data protection issues).

On the other hand, advertising for events and services will be ensured. This would imply that the advertising regulation should be taken into account. Main questions are the following :

- What are the obligations and duties of the advertiser? What information should be integrated in the advertisement ?
- To what extend the advertiser is bound by the content of the advertising ?
- How an advertising can be differentiated from an offer ? What consequences does the qualification of an advertising in offer has on the advertiser?
- What consequences the type of medium used has on the advertiser ?
- What are the rights of the consumers (namely any relevant information enabling the consumer to make up his mind on whether he can benefit from the advertising and decide either to accept it or refuse it — on the basis of an opposition right granted by the advertiser - if he believes that the advertising is useless and intrusive.)

Such analysis should be carried out in the light of the Directive 84/450/EC concerning misleading advertising, of the Directive 97/55/EC on comparative and misleading advertising, of the distance contracts directive, and of the European Green Paper on commercial communications of 1996, whose principles should be resumed in the forthcoming draft directive on electronic commerce.

National regulations are also determinant since they regulate large parts of advertisement matters, such as the price, the free offers, protection of children or other specific groups of population, advertisement for some products, etc_

5. ELECTRONIC PAYMENTS ISSUES

I. Issues common to both applications

The security and payment aspects have been given careful examination in the project outline. It appears that payment systems will not be integrated into the first trial but will in fact enter into the second trial.

There are 3 different models which may potentially give rise to different legal issues. The payment system for the entertainment model provides the fullest details in relation to the payment methods envisaged.

The types of payments envisaged between private clients and the agent are credit card payments using secure encryption methods and the possibility in the future of smart cards.

For the professional client electronic fund transfers using EDI are envisaged.

For the professional client the relationship will be determined by the contractual relationship between client and agent. Payment will involve transferring the amount on a daily basis to the bank using existing payment methods.

The issues which will need to be considered for these models include:

Security requirements

The use of encryption and digital signatures are needed to protect integrity and to authenticate the parties.

The authentication of the buyer and the various methods which can be used to achieve this end have been considered.

There is mention of SSL, SET and OKAPI

The issue of non-repudiation needs to be considered further. Will this be achieved through the use of digital signatures?

Verification of credit card details —will this take place off or on-line?

Data collection

The use of the data should be addressed in relation to Data Protection Regulations (see part on data protection above).

II. For the administrative and legal scenarios

The following questions should be considered :

- What type of payment methods is foreseen?
- Transfer of payment to bank — will this take place electronically? What security methods are envisaged?
- As above encryption and digital signatures?

6. TAXATION ISSUES

The tax issues raised by the TRADE trials cover nearly the whole scope of e-commerce taxation, since the scenarios involve most of the features of common e-commerce schemes. To which extent these issues are really important to the TRADE project depends on several actual facts of the trials which are not identified by the scenario descriptions.

I. Income Tax

It is less probable that the generally discussed income tax issues are of importance for the TRADE project. To surely prevent from constituting a permanent establishment it should be avoided to have an own or rented server abroad. Such a situation should not occur in the trial situation since servers are hosted in Italy and Spain. However, the OECD is already working on that issue. In the near future a server abroad will probably not be regarded a permanent establishment according to the (amended) OECD Model Convention. Selling tickets or especially providing (legal and administrative) services for clients in another country might fall within the scope of withholding tax provisions of the recipient's jurisdiction. Both Italy and Spain have far-reaching national withholding tax provisions. So the bilateral double tax treaty between the trial states must be examined with regard to that point.

A specific point should be regarded with respect to the legal and administrative service scenario. In the "Expected Advantages" section (section 4.3.3.2 of the TRADE Trials Application Scenarios) the possibility of more distributed working is mentioned. This possibility poses problems in the field of (national and international) transfer pricing. Especially in such high integrated transactions over the Internet the applicable method and the way of application are quite unclear. The OECD is working on that issue as well. The OECD intends to amend its Transfer Pricing Guidelines with regard to Internet transactions.

The use of an electronic catalogue as mentioned in the ticketing scheme poses difficult questions in the field of accounting. Who is the taxable owner of the electronic catalogue? Contributions to this catalogue will be made by several organisers. Perhaps the catalogue is composed by the agent or an information broker or by a third party on behalf of an actor in the ticketing scenario. Does the electronic catalogue represent a balance sheet item? An alternative is that such advertising expenditures can be deducted at once from the profit of the year in which they are spent. If the asset must appear in the balance sheet, is it subject to depreciation and, if applicable, to which annual rate?

II. Value Added Tax (VAT)

With regard to VAT one administrative issue is of specific importance for the TRADE project. Although the interface with administration is not a core focus area in the ticketing part of TRADE

(page 23) the invoicing problem is very important for the technical solution. The issuance of a tax invoice is fundamental to the credit invoice VAT system of the Sixth Directive on VAT. It has to comply with several requirements laid down in national law and/ or the tax authorities. Besides the indication of several transaction related data it identifies the output tax liability of the supplier and is mandatory evidence of recoverable input tax by the customer. Paperless tax invoicing through electronic means is regularly not possible according to the national law of the EU member states. A printed invoice must contain certain transaction related data. It must be ensured that these data can be obtained. The Spanish and the Italian national tax law need to be examined.

A key point in the ticketing scenario is the determination of the nature of transactions. Separate place of supply rules apply to goods and services. According to the EU supplies transmitted electronically must be regarded as services. In this case VAT is charged at the supplier's place, the customer's place or the place of performance or enjoyment. Art. 9 of the Sixth Directive determines the exact place of supply. Since the place of supply rules identify the (trial) state where (and to which rate) VAT is charged, this issue needs to be addressed further.

To apply the VAT rules it is necessary to identify the transactions carried out between the participating actors. The trial scenario is not sufficient with regard to this point. Does the agent provide a service at a flat rate for the organiser? Does he get a provision depending on the number of ticket sold. Does the agent himself determines the ticket price and earns the difference? Who is in charge for the setting up and the maintenance of the electronic catalogue and to whom is that service provided for which kind of fee?

In the legal and administrative service trial the application of VAT rules does not provide specific problems with regard to the deployment of electronic means. The trial scenario does not fundamentally differ from a conventional situation. As it is stated in the TRADE Trials Application Scenario the services are developed off-line. Thus, only the means of delivery change. Thus, the place of supply should be determined rather easily.

7. LIABILITY ISSUES

I. TICKETING SCENARIO

Summary of the project

According to the document entitled _TRADE Trials Applications Scenarios" this project sets up a service consisting of a software application that is capable of managing reservation and selling of tickets related, inter alia, to cultural and sportive events. This service is known as service tickets supplier (hereinafter BEL). The software will be located in a server that mainly carries out data server functions. The interlocutors of this application will be the agents (i.e., professional users such as ticket agencies and box offices) who will handle clients' requirements (such as reservations) and consumers' orders.

The agents will be connected to the BEL via an intranet, (i.e., a private net operated by IGN, -IBM Global Network-). Consumers will be connected via an Internet access provider.

The BEL obtains the ticket information from the so-called "event owner" who owns the event. Indeed, the BEL sells the information on behalf of the "event owner".

Defining on-line intermediary roles

The first issue to be clarified is whether on-line intermediary functions are carried out by the different actors of the project. Before doing so, let us define the on-line intermediaries and their functions.

By on-line intermediaries should be understood as being those actors who do not take part in the creation or selection of information to be disseminated. Instead, on-line intermediaries play various roles in the on-line dissemination of information provided by so-called "content providers".

In particular, the different functional roles that can be carried out by on-line intermediaries are basically the following:

- *Network operator*—providing the facilities for the transmission of data such as cables, routers and switches.

- *Access provider*—providing access to the Internet. Users connect to the Internet through their access provider's server. Commonly, an access provider also provides an e-mail account.

- *Host service provider* — providing a server upon which it rents space to users to host content, for instance a web page, which can incorporate all kinds of material (such as software, text, graphics, sound).

- *Bulletin board operators, news groups and chat room operators*—services providing space for users to read information sent by other users and to post their own messages. Usually, they are devoted to specific topics. There are two types of newsgroups: moderated and unmoderated. The chat room allows direct communication in real time.

- *Information location tool providers* — providing tools to Internet users for finding web sites where information they seek is located (such as Yahoo!). There are two types of search engines, namely automated search engines and search engines that rely upon human beings to review and catalogue web sites.

Functions: the server and the network

From the description of the Trade project, we can identify two functions that, a priori, could fit into the roles carried out by on-line intermediaries: the server function carried out by the BEL and the private network that connects the BEL to the agents operated by IBM.

The server function provided by the BEL

As regards as the server, owned and managed by the ticket service supplier (BEL), it should be noted that it does not provide host facilities but it is only employed to run the application owned by BEL. Thus, BEL, by providing a server to run the application is not a host service provider or any other type of on-line intermediary and, therefore, if third party complaints for hosting copyright material without the copyright holder's authorization or for hosting defamatory material were filed, damages should not be granted[18]. It is an entirely different issue whether BEL, by providing as well the application, will bear that risk (see below).

[18] The types of substantive law more likely to be infringed by using on-line facilities include the following:
Copyright material—The infringing act may occur when certain files containing copyright material such as text, pictures, or sounds are posted on a web page from which they may be downloaded all over the world.

The network operated by IBM

As far as the private network is concerned, indeed, the operator of the net should be aware that it could bear the consequences of third parties' complaints for transmission of illegal material. However, so far, both case law and existing legislation on service providers' liability have exonerated the network operators from liability for actions initiated by others (such as for carrying illegal information which was put on the network facility by an user). This is the case of the US Telecommunications Act and the Digital Millennium Act which both exonerate network providers from liability. At the European level, it should be noted that Article 12 of the Draft Proposal for a Directive on electronic commerce establishes the following: Member States shall provide in their legislation that in the case of the provision of a service in the Information Society consisting: (a) in the transmission, on a communication network, of information provided by the beneficiary of the service; or (b) in the supply of access to a communication network, the liability of the provider of such a service for the transmitted information cannot be invoked, except in the context of an cease and desist order under condition that the provider (1) is not the originator of the transmission, (2) does not select the addressee of the transmission, and (3) does not select the information that is transmitted. Based on the above provision, to the extent that the IBM network as transmitter of information fulfils the conditions (1) (2) (3) will not be responsible for damages although an injunction (the network provider is ordered to stop carrying certain information) remains possible.

Despite the above considerations, it is likely that in the contract between BEL and IBM for the purposes of leasing the net, IBM will try to include a clause exonerating itself from liability for the illegal and harmful information it carries. BEL (provided it has the necessary bargaining power) should try to avoid including and accepting such clause.

Identification of contractual liability issues

Identification of different roles and participants

Besides the question of extra-contractual liability issues of on-line intermediaries addressed above, the different actors of the Trade project will need to enter contractual agreements to establish the legal framework which will govern their relationships. Within these agreements, clauses regulating liability will certainly need to be included. Let us first enumerate the main participants in the project:

- BEL (Tickets service supplier)
- The owner of the event
- IBM (supplying the private network)
- The agents
- The consumers

Illegal and harmful content—The infringing act may occur when material such as pornographic, racist or terrorist materials are disseminated via Internet facilities.
Private and defamatory material—Private material such as pictures taken in intimate situations could be posted on web pages, bulletin boards, chat rooms, etc., and made available to users, infringing therefore rights of privacy, including those contained in European data protection laws. The same may occur with defamatory material.
Trade secrets.—It may happen that employees disclose confidential information which may be used in a trade or business and which is not known in that trade or business.
Misrepresentation—This may occur when false or incorrect information provided by someone and disseminated using on-line facilities causes damage to a third party.
Others—An intermediary could also be held liable for the infringement of other substantive laws such as patents, trademarks, and unfair trade practices.

- The bank

Need to sign up contractual agreements

The above participants need to sign contractual agreements. In particular, the following contracts should be entered into:

- First, BEL has to sign an agreement with the owner of the event.- To the extent that BEL does not buy the tickets but only acts as an agent of the owner of the event, by promoting, distributing and concluding offers on behalf of the owner of the event, the contractual relationship between the BEL application and owner of the event can be classified as an agency. The agency is regulated by the Directive 86/653, 18 December 1986.

  This contract will establish the duties and obligations of the owner of the event and BEL. In addition, BEL may want to introduce clauses exonerating itself from liability.

- Second, BEL has to sign an agreement with the agents. To the extent that the agents will buy a number of tickets to resale to their clients, this agreement will include duties and obligations of both parties. In addition, exonerating clauses may be included.

- Third, the BEL has to sign a leasing contract with the network provider (IBM).

- Fourth, the BEL will sign a contract with the consumer when it orders tickets. This will be a typical electronic contract[19].

- Fifth, the BEL has to sign up a contract with the bank[20].

Content of the contractual agreements: liability clauses[21]

Agreement between BEL and the owner of the event.- Concerning liability clauses to be included in this contract, BEL should consider the adoption of the following clauses:

The owner of the event has the obligation to clear the copyright of the material that is sent to the BEL application (such as pictures accompanying the tickets). If the owner of the event fails to fulfil this obligation and BEL is sued, the owner of the event will pay the damages to restore BEL application to its position.

The owner of the event has the obligation to fulfil the obligation it has engaged to when selling the tickets. If the event is not performed and the BEL was sued, the owner of the event will pay the damages to restore BEL to its position.

Failure to perform BEL obligations vis-‡-vis the owner of the event will not arise indirect or consequential damages.

---

[19] This paper does not address this type of contract because this issue falls into the area where the CRID (Anne Salaun) is competent.

[20] This paper does not address this type of contract because this issue falls into the area where the QMW is competent.

[21] This paper does not address other types of contractual clauses because this issue falls into the area where the UIB (University of Balearic Islands) is competent.

Agreement between BEL and the agents.- Concerning liability clauses to be included in this contract, BEL should consider the adoption of the following clauses:

BEL is not liable for any loss or damage suffered by the agent caused by any delay or failure to perform when it is caused by an impediment beyond control such as a breakdown of the private network which links the agents with BEL.

Failure to perform BEL obligation duties vis-‡-vis the agents will not arise indirect or consequential damages.

II. LEGAL AND ADMINISTRATIVE SCENARIOS

These two scenarios are very similar and accordingly will be dealt together.

Summary of the project

According to the document entitled _TRADE Trials Applications Scenarios" this project sets up an application which sits in a server. The server contains a database of lawyers/consultants specialized in different areas. Upon request from a customer, the server will provide a lawyer/consultant. The customer may require the services of the lawyer to handle its case before the court. In order to do so, the lawyer will communicate with several actors such as the court, notaries, administration by electronic means. In particular, all the documents will be transferred using the server.

The functions

From the description of the legal scenario, it appears that none of the participants in this scenario plays a role of on-line intermediary.

In this scenario, it seems that the service provider (who runts the server and the application) plays a role of information provider and agent, in a similar way as described in the entertainment scenario. In any event it will not be classed as a host service provider because it does not rent space to users. Therefore, no issue arises concerning on-line intermediaries' liability.

8. PRIVATE INTERNATIONAL LAW

Since electronic commerce might involve parties situated in different countries, it is easy to imagine that cross-border conflicts may arise. For this reason, issues of private international law will have to be discussed. As our contribution to the TRADE project is only meant to be rather brief, we will not have the time to address all issues of private international law, that the project may imply. Consequently, this report will only concentrate upon some central issues of private international law.

I. Contract obligations.

The most important questions that need to be explored from a private international law point of view, lies within the field of contract law. The main problem is identifying the law applicable (lex causae) to the contract in question. Here, the 1980 Rome Convention on the law applicable to contractual obligations will be of great significance. Firstly, one will have to identify the law applicable to determine the existence of a legally binding contract. Secondly, one will have to

determine which rules that are going to govern the contractual relationship. Finally, one will have to analyse whether there exist mandatory rules or similar which may limit the use of the law applied.

Within the field of contract law, one will also have to develop a discussion concerning which law that governs the question of what the effects of the use of digital signatures shall have.

II. Consumer protection.

While the previous questions mainly address business-to-business problems, the contracting will also imply the discussion on consumer protection. The EC has in recent years been more and more concerned with the issues of consumer protection, and consequently, issued several Directives addressing these issues. In a contractual situation a business-to-consumer relation will address issues concerning mandatory rules. In a context of private international law, there are therefore several points that have to be discussed.

III. Data protection.

This would imply identifying the law applicable (lex causae) to the data processing taking place on the basis of the contractual agreements. It is presumed that the processing of personal data often will take place at the sites of both (or more) parties to the contract. The data in question may be communicated from another country through the Internet. Data mining may be included in this perspective.

ECLIP can only offer a general discussion on the choice of law, disregarding the aspects of public law. The main issue will be the EC-Directive on data protection, and its applicability.

IV. Intellectual property right.

The task here is to identify which country's law will govern the question whether a copyright infringement has taken place or not. Here, the Bern Convention will be useful.

V. Other Issues

Finally, E-CLIP can also seek to straight out some interlegal issues concerning liability for misleading information and security requirements.

VI. Delimitation of the project

This report concentrates upon matters of private law. As far as possible, matters of public law, like tax law etc., will be left out of the analysis.

Furthermore, we will presume that the contracting are taking place between European parties only. Consequently, it is a study of the private international law within Europe that will be developed. The rules of private international law outside Europe will not be addressed.

III. LEGAL ISSUES OF THE TRADE SERVER

1. Introduction

The operation of the TRADE server is likely to raise specific legal issues, different from that arising in the applications. Nevertheless, such issues will greatly depend on the level of autonomy of the TRADE server related to the pilot applications. Indeed, in some cases, there is no clear line between some technical features between those offered by the common server to all applications and those specific and integrated in the pilots themselves. This is namely the case of electronic payment systems which could be a sspecific feature of the TRADE server or not.

However, we could infer from the documents submitted to us by TRADE that the project will mainly focus on the trials applications. Therefore, we will restrict ourselves to address those legal aspects necessarily implied by the design and operation of the TRADE server as such. Some other aspects could be very similar to those developed in the second part relating to the applications.

2. Analysis of the nature of TRADE server

It is particularly important to consider the role of the TRADE server in a electronic commerce transaction and the consequences thereof. The first issue to be considered is whether the server falls in with the definition of an "on-line intermediary". It is said later on that on-line intermediaries could be defined as actors who do not take part in the creation or selection of information to be disseminated. Instead, on-line intermediaries play various roles in the on-line dissemination of information provided by so-called "content providers".

The TRADE server plays some functions of intermediary between the sellers and the buyers, for instance by offering electronic payments systems, security platform or anonymisation firewalls. As to whether such functions could qualify the role of TRADE server as an on-line inetremediary should be addressed. The consequences of such a qualification are particularly relevant for the matter of liability for content delivered through the TRADE platform.

3. Legal issues of technical solutions adopted by the TRADE server

3.1. Access control mechanisms

Access controls systems, which can cover set-top boxes for web access from a TV set and any other access systems, are liable to raise three main legal aspects. On one hand, the identification of the user on which is based the authorisation of access will probably be digital signature mechanisms certified by Trusted Third Parties. Therefore, the competent legislation on electronic signature should be taken into account.

On the second hand, a legal protection of conditional access services is currently under development at an European level. Indeed, a Proposal of Directive on the legal protection of conditional access services aims at prohibiting some commercial activities of manufacture, import, sale etc... of any equipment or software designed or adapted to enable the unathorised access to a protected service. Such a protection is really relevant when launching an InformationSociety services - which are expressly covered by the Draft Directive- based on conditional access. Therefore, a proper consideration of this aspect should be carried out by the TRADE partners.

A third aspect is data protection regulations, since such access systems and other security tools developed by TRADE server aims namely, acoording to techical annex, at the authentication of buyers. Therefore, a great number of personal data will be collected and processed by the server itself which entails a necessary compliance with data protection principles, which are explained in details herafter in Title II.3. Particularities of TRADE server should be however considered, namely as regards to the identification of the legitimate purpose of the collect and processing of data and the identification of data controller upon whom sets a number of obligations.

3.2. Payment Gateway

In the case where the payment systems are offered and monitored by the TRADE platform, the legal issues related to electronic payments should be addressed at this stage. We refer for a short explanation of those aspects to the title II.5. hereafter developed with regard to pilot applications.

3.3. Anonymisation Gateways

It is said in the technical annex of the TRADE project that some tools for enhancing the confidentiality and data integrity might be integrated in the server, such as -I quote- 'virtual private network' and 'tunneling protocols'. In this case, a great number of personal data related to users and buyers will be collected at this stage and kept by the TRADE server in exchange of an anonymised identification.

Therefore, for this specific data processing carried out in the process of anonymisation, the operator of the TRADE server might be considered as the controller. It should be reminded that the Directive on the protection of personal data defines the controller as the "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the means and purposes of the processing of personal data". In this case, the obligations laid down by the directive should be complied with by this controller, i.e. the person responsible for the TRADE server of the determination of the means and purposes of the anonymisation.

For these obligations, we refer to the part on data protection developed relating to pilot applications under Title II. 3.

3.4. Microsoft Transaction Server

The utilisation of a tool such as the Microsoft Transaction Server might bring important issues, since this system is primarily designed to comply with US legislation. Therefore, the Mlicrosoft system should be considered so as to enable European transactions and to adapt it to the European regulatory framework.

Just two examples can be considered here. Firstly, the technical annex states that such Microsoft tool enables the calculation of sales tax. This notion is very characteristic of the US taxation regulatory framework and does not exist in European taxation systems. As a consequence this feature of the Microsoft Server is completely useless when a transaction is carried out at an European level. At the contrary, the VAT has to be charged upon European transaction. Therefore, an analysis of the VAT systems in Europe should be taken into account and integrated in the server used by TRADE so as to replace the US sales tax calculation.

Another example is the functions of ordering and choosing a shipping option. If a consumer is involved in such a process, a number of important regulations, such as the European Directive on consumer protection in Distance contracts should be complied with. We refer on that point to the analysis of consumer protection developed for the pilot applications under Title II.5 of this document.

4. Applicable law and jurisdiction

The intervention of a TRADE server between the buyer and the seller could mix up the normal application of rules determining the applicable law and jurisdiction to an electronic commerce transaction. Therefore, a particular attention should be devoted to the intervention of the TRADE server when analysing the applicable law to any legal consequences of a transaction entered in the framework of an application.

Besides, the aspects of applicable law and jurisdiction of the legal issues specific to the TRADE server, as exposed hereabove, should be considered.

CONCLUSION

After having drawn the main legal issues relevant for the first two TRADE applications and TRADE server, we could plan the further assistance that ECLIP could provide , as follows :

Fields of law to be considered (to be agreed upon with TRADE coordinator):

- **Contract Law**

  ⇒ Further analysis of the legal framework of the digital signature

  ⇒ *Manpower needed* :to be estimated if further assistance is needed on that topic

- **Intellectual Property Rights**

  ⇒ General issues of IPR in an on-line environment

  ⇒ Specific IPR aspects of the multimedia catalogue of events developed in the ticketing scenario

  ⇒ *Manpower needed* : Since TRADE does not intend an on-line dissemination of copyrighted materials, most of the questions mentioned above will be rather easy to answer. Thus, it should be possible to do the assistance work within 5 man-days. In case that TRADE wants ECLIP to analyse which of the pictures, texts and video clips used in the web site, especially in the multimedia catalogue, the number of man-days has to be augmented.

- **Data protection Law**

  ⇒ Analysis of the TRADE scenarios from a data protection point of view (identification of types of data, of controller, of obligations and principles applied in TRADE applications) : this analysis has been already largely done in this paper. E-CLIP could nevertheless answer to any other specific questions.

  ⇒ Analysis of the application of data protection principles to the operation of the TRADE server.

  ⇒ *Manpower needed* :to be estimated if further assistance is needed

- **Consumer Protection**

  ⇒ Further analysis of Distance Contracts Directive 97/7/EC and the Council Directive 93/13/EC on unfair contract terms in consumer contracts and assistance for transposing principles thereof in TRADE applications

  ⇒ Further analysis of Commercial communications and advertisements regulations

  ⇒ analysis of the consumer protection issues arising by the operation of the Microsoft Transaction Server (if integrated in the TRADE server)

⇒ *Manpower needed :* 14 man-days

- **Electronic Payments Issues**

⇒ For payments it will be necessary to have more detail as to the methods considered and their implementation in relation to the models. Since payments will not be introduced until the second trial perhaps this area of assistance can be provided when fuller consideration of the methods to be used have been decided.

⇒ *Manpower needed :* to be estimated when assistance will be needed (according to the stage of development of payments methods)

- **Taxation Issues**

Income Tax :

⇒ withholding tax provisions and analysis of double tax treaty between Italy and Spain

⇒ Transfer Pricing applicable to TRADE on-line applications

⇒ Issue of electronic catalogue relating to accounting regulations

VAT :

⇒ issuance of tax invoice

⇒ nature of transactions in the ticketing scenario

⇒ analysis of the VAT issues so as to replace the calculation of sales tax provided by the Microsoft Transaction Server (if integrated in the TRADE server)

⇒ *Manpower needed :* The assistance to TRADE makes it necessary to closely examine specific provisions of national tax law and provisions of the Italian-Spanish double tax. Thus, the assistance will probably require about 8 man-days. For the last point (Microsoft Transaction Server) : 6 man-days

- **Liability Issues :**

⇒ The main liability issues of intermediaries have been considered in this paper. Nevertheless, E-CLIP could examine in further details some specific issues if needed.

⇒ *Manpower needed* :to be estimated if further assistance is needed on that topic

- **International Private Law**

⇒ Applicable Law to contracts entered in TRADE applications

⇒ Applicable Law to digital signature

⇒ Applicable Law to data protection

⇒ Mandatory provisions for consumer protection

⇒ (If needed, the determination of the law applicable top copyright infringement and security requirements can be considered as well.)

⇒ *Manpower needed :* 12 man-days

ANNEX 5 : Assistance to TRIP : List of questions asked by TRIP co-ordinator

ESPRIT Project 25594

Travel Reservation and Interactive Purchase

RTD in Information Technologies

Domain 7: Technologies for Business Processes

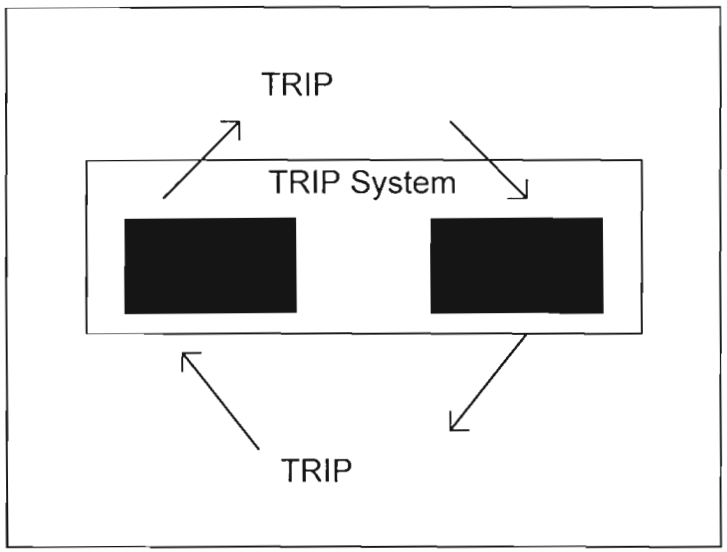
Task 7.10 Electronic Commerce

T5.6 Liability Issues relating to TRIP

Reference : 25594/
Version A
Date : 98/8/3

1. TRIP LEGAL ISSUES

The TRIP system facilitates Travel Agents with access to information and booking facilities for products and services supplied by the TRIP Operator. The system is designed so that agents can enter their customers requirements such as dates, service required etc. and then search for relevant products a list of suitable items is returned . On selection of an item agents move from a connection to the TRIP Engine to a direct connection to the TRIP Operators system to access product information and secure products.



The origin and flow of data held on TRIP databases

The TRIP Agent supplies the TRIP Operator with their customers details which are stored on the TRIP engine along with details of the products and services that have been purchased.

For the purposes of this document the body that will be formed to market and provide access to the TRIP system is referred as TRIP Inc. This document assumes that a contract will exist between TRIP Inc. and TRIP Operators and between TRIP Inc. and TRIP Agents for the pilot and later deployment of TRIP. The pilot study will involve TRIP Agents in the UK and TRIP Operators in France, Italy and Portugal. Later deployment of TRIP will involve the rest of Europe.

International and National Law

No	Issue	Notes
1.	Which national and international laws relate to the sale of travel services and are the any special provisions regarding electronic sales?	Which laws are relevant for on-line transactions to sell products, conduct business or provide customer services? What jurisdiction would apply in event of dispute between parties in different countries ? Is any over-riding legislation which might invalidate a contract such as Consumer Protection Legislation ?
2.	Do any European Travel Associations have any rules that would affect TRIP ?	IATA, ABTA, Civil Aviation (Air Travel Organiser's Licensing) Regulations 1995 [ATOL], The Package Travel, Package Holidays and Package Tour Regulations 1992 will apply.
3.	Eligibility to conduct business in different countries.	Some travel companies may only be authorised by their bonding companies or licence to conduct business in particular countries so before entering into a contract a TA will need to establish whom the purchaser is and where they are located .
4.	What licensing is required by TRIP and TRIP	

	Operators , do vendors have to be licensed? Is TRIP Inc. considered a vendor?	
5.	Are there any national laws that relate to the language in which information is presented.	There is need to determine in what languages information will need to be available on the Server and who will be responsible (if anyone) for translation of input and output dialogue, in all its forms, into the language(s) of the target market.
6.	What are the rules governing the display of Currencies and Conversion Rates.	Acceptable rules concerning currencies displayed and conversion rates to be applied may need to be specified.
7.	How does the Euro affect TRIP? • Prior to conversion • During conversion of both countries in a transaction • During conversion of one country in a transaction • After conversion by both countries in a transaction • After conversion of one	Euro Currency is due to be introduced progressively from 1.1.99 (Banking possible) 1.1.2002 (Currency is In circulation) although the participating countries have still to be announced. How is TRIP affected by conversion to the Euro in participating countries.

	country in a transaction • Should we have an operating company in a Euro based country?	
8.	CRS status	Is TRIP considered a computer reservation system in terms of European law - do we need to follow rules to ensure that screens are not bias in favour of a particular operator ?

Electronic Contracting

9.	What are the laws governing electronic contracting ? What do we need to put in place to enable it ?	Traditionally such an agreement would take the form of a printed document signed by both parties but an electronic document maybe an option and would certainly speed up the process of bringing new Agents and Operators on-line. It is necessary to ensure the relevant clauses are present in the appropriate contracts to reduce the liability of TRIP Inc., partners and licensees.
10.	When does a contract exist ?	How are offers and acceptances communicated ? When does the exchange of electronic messages become a binding contract - when booking ended or when payment is sent or received ?
11.	Service Provision & Availability	Internet Access Providers will be expected to manage peaks and troughs in bandwidth ; monitor activity; minimise time off-line for maintenance, software updates, etc. Sites should otherwise be available 24 hours per day, 7 days a week, 365 days per year. TRIP Operators will be required to provide access to data, availability and booking facilities for specified periods. Agreement between TRIP INC. and TO's who act as IAP's will need to spell out obligations

Liability

12.	Who is liable if payment is sent but not received?	If the agent sends payment but it is not received by the TRIP Operator who is liable ?
13.	Who is liable if a service or product is not delivered - who guarantees the product? What if the traveller is not satisfied with the product when they arrive ?	TRIP must exercise care to ensure that it is not held liable for the actual quality of the product or service being advertised.
14.	Liability for advertisements on the site.	What national and international laws govern relate to advertising standards and what needs to be done to ensure we comply?
15.	Fraudulent bookings	Should we include a clause in TRIP Agents contract/disclaimer to guard against bookings created for fraudulent purposes.
16.	Employee Liability	Can a business can be held liable for the acts of its employees in the course of his / her employment.
17.	Liability for customer data	Any data taken from TRIP Agents or their customers is subject to the Data Protection act in the UK. What relevant legislation exists in other partner countries?
18.	Prevention of fraudulent, defamatory or obscene material from the TRIP Operator	As information accessible through TRIP is provided by a third party (TRIP Operators) do we require a clause in contracts stating that the inclusion of libellous, or inaccurate, or information published for fraudulent purposes would result in the termination of the agreement? What is the liability of TRIP for information accessible through the TRIP system? Should we publish a disclaimer on the site limiting our liability would this be suitable for

		different participating countries?
19.	Discrimination	Ensure that TRIP participants do not handle, publish or facilitate access to any information that discriminates, or encourages discrimination against any person on : • the grounds of gender or sexual orientation • racial or ethnic grounds or that tends to incite racial hatred Do we need a contract clause to guard against this?

Taxation

20.	What determines how VAT is calculated ? Whose responsibility is it to ensure that the correct VAT is collected? What is TRIP Inc's. responsibility ?	Information so far indicates that the VAT paid is determined by the laws of the country where the vendor resides. In this instance is the vendor the TRIP Operator or TRIP Inc.?

IPR

21.	Protection of system name ?	Although the system is called TRIP presumably this may need to change if it infringes an existing product name. Is this only if it is a similar type of product? The systems name and logo need to be registered as a trade mark in all the territories in which we wish to trade is there a body where a name can be registered for the whole of Europe?
22.	Protection of the TRIP system and software from	Who owns the system and what are rights relating to licenser and licensee?

	copying and interference ?	
23.	Registration of Web Site(s) and Domain Names?	TRIP INC. and URL's may need to be registered. Each TRIP Operator may need to register Domain name / URL.
24.	Can TRIP as a whole or parts within TRIP be patented ?	Would we be liable if we did not register a patent ? Does a patent already exist that specifies a TRIP type system or elements used within the TRIP system. What options do we have if a patent does exist i.e. fight it or pay royalties.
25.	Copyright of software and information in databases.	In the UK are computer programs are protected by copyright? What about the rest of Europe? Can copyright be used to protect databases?
26.	Copyright in TRIP Data / information. Ascertain position on Translation Rights. In the UK is copyright granted automatically by legislation at the point of creation so there is no need to apply for it.	A single World Wide Web page can contain literary, artistic and musical works involving dozens of different copyrights each requiring the consent of the copyright holder before they can be used.
27.	Who owns copyright in a Web Site ?	Are web pages subject to copyright ? Who owns the copyright if the site is designed by a designer specifically engaged to create it. Do we need to ensure that any contracts awarded to designers for creation of new web sites / pages include a clause obliging him/her to assign copyright to TRIP ? What steps do we need to take to protect copyright such as including a copyright notice on the site ?
28.	Hyperlinks and Gophers	What are the rules relating to hypertext links to other documents?

29.	Copyright Infringement - Caching ?	Is caching a web page an infringement of copyright ?
30.	Copyright Infringement ?	It has been suggested in legal circles that System Operators(SO) such as Netcom should be held strictly liable for any copyright infringement by their users, whether or not they were on notice of such infringement or took reasonable steps following such notice. SOs have argued that they are mere carriers and despite their need to reserve some control over the material published on their systems cannot monitor all on-line activity and should not have any liability for users actions. A recent case in the US suggested that a SO may be liable for contributory infringement, but only after being put on notice of an infringing file and, only then if the SO failed to take reasonable action. It still leaves open the question of when notice is ' reasonable' and what actions must be taken once prima facie infringement has been shown. What would be the position of TRIP?

Consumer Protection and Privacy

31.	Official Secrets Act	Unlikely to apply but it is essential to conform with the provisions of the Official Secrets Act 1989 in the UK which carries heavy penalties. Extreme caution must, therefore, be exercised before handling, displaying, or otherwise making such material accessible on an electronic information system. Is there similar legislation in rest of Europe that would be relevant?
32.	Is it necessary for the	If the TRIP Agent is not advised that it is his responsibility to make the customer aware of

	traveller to be aware of the disclaimer that the TRIP agent has agreed to. What are the obligations of TRIP?	any disclaimer agreed to on the customers behalf is the disclaimer valid
34.	Disclosure of confidential information relating to TRIP by a TRIP Agent or TRIP Operator.	Do we require a contract clause to guard against this?

ANNEX 6 : Assistance to TRIP : First set of answers

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

ELIP
Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

Taxation, Intellectual Property Issues and Data Protection Issues Relating to TRIP

ITM , CRID

CONTENT

1 Taxation, No. 20

1.1 What determines how VAT is calculated?

The applicable VAT provisions of the country where the supply takes place. Since all EU Member States amended their national law in accordance with the Sixth Directive on VAT the reference to its provisions should generally be sufficient. Specifics of national VAT law will be added if necessary.

Since their is no supply of a journey all transactions performed with respect to a journey must be regarded separately, e.g. accommodation, meals, transport, car rental. In general, all these transactions qualify as services according to Art. 6 par. 1 Sixth Directive.[1] Such supplies of services may be taxable at the place, where the real estate is situated, Art 9 par. 2 lit a) Sixth Directive (accommodation),[2] where the transport takes place, Art. 9 par. 2 lit. B) Sixth Directive,[3] or where the supplier has established his business according to Art. 9 par. 1 Sixth Directive (meals).[4]

Art. 26 Sixth Directive derogates from these general rules for travel agents or tour operators, who deal with customers in their own name and use the supplies and services of other taxable persons in the provision of travel facilities. Travel agents acting as intermediaries are therefore excluded from the derogation, Art. 26 par. 1 2nd sentence. According to Art. 26 par. 2 Sixth Directive all transactions performed in respect of the journey shall be treated as a single service and be taxed at the place of the supplying travel agent/ tour operator. Taxable amount is the margin, i.e. the difference between the price paid by the traveller and the travel agent's/ tour operator's cost of supply and services from provided by other taxable persons. Such (single) journey services are excluded from the right of deduction.

In the commercial environment of TRIP different scenarios might appear:

1) Generally, the TRIP agent will act as an intermediary on behalf of the appropriate operator for a booking provision or another kind of remuneration. Assuming this, the TRIP operator deals with the customer in his own name. As all the other requirements of Art. 26 Sixth

[1] E. g. ECJ Decision of 2 May 1996 C-231/94 regarding meals.

[2] Langer Commentary on Sixth Directive. In: Reiß, Krauesel, Langer. Umsatzsteuer (VAT) Bonn, 1998. Art. 9 note 27.

[3] Id. note 28.

[4] ECJ Decision of 2 May 1996 C-231/94.

Directive should regularly be met the place of supply is the place, where the TRIP operator runs his business or maintains a fixed establishment, here in Italy, France or Portugal. Taxable amount is the margin as defined above. According to French national law the provision paid to the TRIP agent reduces the margin, which is usually not the case.[5] The TRIP agent's liability to VAT must be determined according the national VAT law of the same Member State according to Art. 28b (E) par. 3 Sixth Directive. Since TRIP Inc. does not yet provide services for remuneration no tax liability is assumed.

2) Where the TRIP agent deals with the customer in his own name, Art. 26 applies to him. The TRIP operator is then taxed according to the general rule with regard to each single service provided. Same applies to previous suppliers (operators) in a chain.

1.2 Whose responsibility is it to ensure, that the correct VAT is collected?

Generally the taxable person carrying out the taxable transaction is liable to pay VAT according to Art. 21 par. 1 lit a) Sixth Directive. Art 21 par. 1 lit. b) allows the Member States to derogate from this general rule with regard to specific services. In such cases the recipient is liable to pay VAT. Member states may require, that supplier and recipient shall be jointly liable. In Scenario 1) the TRIP operator might be liable to pay the tax for the TRIP agent as far as national law provides for such derogation.

1.3 What is TRIP Inc's. responsibility?

In the future TRIP Inc. will be required to pay tax on services provided to TRIP agents and TRIP operators in exchange for remuneration. The determination of the tax payable will depend on the services supplied.

To enforce taxes in the environment of electronic commerce German financial authorities tend to focus on intermediaries (often referred to as trust centres) to gather information and to pay taxes. Such duties might be imposed on TRIP Inc. The development in this field should be watched closely.

[5] Rädler, Albert J.; Lausterer, Martin. Margenbesteuerung von Leistungen der Reiseveranstalter in der EG, Umsatzsteuer-Rundschau (UR) 1995, page 285, 291.

2 Intellectual Property Rights, No. 21 - 30

2.1 Protection of the system name (No. 21)

2.1.1 Although the system is called TRIP presumably this may need to change if it infringes an existing product name. Is this only if it is a similar type of product?

The system name would need to be changed if it infringes an existing trademark. According to Art. 5 (1) (b) of EC Directive 89/104/EWG from 21 December 1988, which is harmonising the national trademark laws and which has been implemented in every member state of the European Union, the owner of a trademark can prevent any third party from using "any sign where, because of its identity with, or similarity to, the trade mark and the identity or similarity of the goods or services covered by the trade mark and the sign, there exists a likelihood of confusion on the part of the public, which includes the likelihood of association between the sign and the trade mark." This means that usually the type of product needs to be a similar one. The directive, however, provides the member states with the possibility to set up a different rule for signs which have "a reputation in the Member State and where use of that sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the trade mark" (Art. 5 (2) of 89/104/EWG). Most of the member states with the exception of Austria and Spain have included such an extension of the protection for marks with a "reputation" into their national trademark acts. Additionally, there are also extension provisions in international treaties. Art. 16 (3) TRIPS (Trade related aspects of Intellectual Property rights) foresees an extension of the protection of notorious marks in certain cases of non-similarity of the products or services - a requirement which so far has not been implemented in the British and Irish trademark acts.
As the concept of protecting well known or trademark with a reputation also outside the similarity situation there is not yet a lot of jurisprudence helping to identify trademark which benefit from these extensions. But the requirement of being well-known or other qualitative criteria will probably be quite high. So, if there is no other known mark identical or closely similar to the brand name you intent to chose, there is probably no other mark of high reputation outside your business area whose rights could be infringed.

2.1.2 The systems name and logo need to be registered as a trade mark in all the territories in which we wish to trade is there a body where a name can be registered for the whole of Europe?

It is possible to register a Community trade mark. The possibility to register a unique trade mark which protects the registered mark in every country of the European Union was created the Regulation on the Community trade mark (Reg 40/94) in 1993. The office registering this trademark is the Office for Harmonisaton in the Internal Market situated in Alicante, Spain. Applicant should use the Standard Application Form which is made available by the Office and which may be obtained free of charge from the Office or from any other industrial property office in one of the member states of the European Union. The Community Trademark will only be registered (with very few exceptions), if there is no obstacle for registration in any of the European Countries. It is not possible to limit the Community mark to only some countries.

One possible obstacle to the registration of the name "TRIP" as a trademark should, however, be considered. It might not only hinder the registration of the name as a Community Trademark but also the registration of the name in any other country of the European Union.

Art. 7 (1) of Reg 40/94 contains certain grounds of refusal for registration, two of a which are in subsections c and d: "trade marks which consist exclusively of signs or indications which may serve, in trade, to designate the kind, quality, quantity, intended purpose, value, geographical origin or the time of production of the goods or of rendering of the service, or other characteristics of the goods or service" and "trade marks which consist exclusively of signs or indications which have become customary in the current language or in the *bona fide* and established practices of the trade". The same wording is used in Art. 3 (1) (c), (d) of EC Directive 89/104/EWG, which means similar grounds of refusal have been implemented in all member states of the European Union. The term "Trip" being used in the common language might fall into one of these grounds of refusal, especially for the kind of service that shall be offered using the name, a travel/trip arrangement service. This problem might occur especially in English speaking countries, but as the word "trip" is commonly known in almost very other European country it might be an obstacle to registration in those countries as well. It might therefore be recommendable to chose a name which does not exist in the common language or at least does not describe the service. The question, whether the name "Trip" can be registered (at least in the form of the logo (combination mark), including the special design of the "T" in the form of an air plane, can, however, not be answered definitely and should be regarded more carefully, maybe with the support of a local lawyer

2.2 Registration of Web Site(s) and Domain Names? (No. 23)

TRIP INC. and URL's may need to be registered. Each TRIP Operator may need to register Domain name/URL.

It is presumed that the question of registration does refer to a possible registration of the domain or URL as a trade/service mark and is not refering to the registration at the different Network Information Centres (NIC), which is first of all a contractual question and does basically not have a effect on trade mark rights. The NICs do not grant any sort of intellectual property rights.

It is possible to register a domain name as a mark if the domain name identifies a product or service, not if it is only used as a pure address of a website without product/service identifying character. If the domain name chosen is identifying the service offered on the website, it can be registered. For the registration of the "Trip"-service a registration in class 39 - packaging and storage of goods, travel arrangement - (according to the Nice agreement recommending a common classification system). The TLD of the domain name is considered to have no distinctiveness. The domain therefore needs to receive its distinctiveness from the second or in the UK and in other countries using an equivalent domain registration system the third level domain. The UK patent offices published the rules according to which they register or refuse registration of domain names on their website (with the exact URL: http://www.ukpats.org.uk/snews/notices/tmnames.html) For further information on the registration of domain names please have a look at the declaration of the US Patent and trademark office (http://www.uspto.gov/web/offices/tac/domain/tmdomain.htm). The rules set up by the US PTO correspond to the rules which most European trademark offices will probably apply accordingly as it is in accordance with the national trademark laws and the Community Trademark Regulation.

2.3 Patentablity of TRIP (No. 24)

2.3.1 Can TRIP as a whole or parts within TRIP be patented?

This question is difficult to answer. As regards national patents the answer depends on the different national laws of the EU member states; as regards an EU-wide patent the solution has to be found in the European Patents Convention from 1973. The national and the European stipulations on patentabile matters are very similar to each other, but non of them contain clear stipulations onthe protectability of software. Neither national patent offices nor courts

have developed clear rules or definitions for this question. Further on, there seems to be a tendancy in favour of a wider protection of software by patent law. It is therefore difficult to predict the future national or international jurisdiction. Finally the protection of software depends on technical charcteristics that we don't know in detail. Thus, only a national patent agent who knows the technical details can give a reliable answer to the question.

However, as far as we can see the patentability of TRIP as a whole and of its elements is very unlikely.

TRIP as a whole is in brief description a new service concept and focuses on reservation, marketing and support issues rather than on technology development. According to Art. 52 (2) Number c) European Patent Convention schemes, rules and methods for doing business cannot be patented. Therefore, the TRIP concept is clearly excluded from patent protection.

Regarding the given *elements of TRIP*, as there are the "multimedia search engine", the "reservation and information system for the storage of data and the management and selling of inventory", the "Interfaces to other reservation systems " and the "Electronic commerce component", the legal situation is less clear. The European Patent Convention states in Art. 52 (2) Number c) that "programs for computers" cannot be patented[6]. This means at first sight that protection of computer software comes not under patent-law. Thus, the concrete software never is protectable. However, the underlying principles and the rules behind this software might be protectable.

An imortant prerequisite for patent protection is the technical character of an invention. Technical character means that the invention has an effect on natural forces. If an invention only influences human imagination it has no technical character. Therefore, software that is to be used on personal computers usually is not patentable. It normally influences only the user's imagination, but no natural forces. But in certain cases software can have the necessary impact on the physical world: This is the case when it is used to steer automatically a technical system like for example an anti-lock breaking system. It is also the case when it hase an influence on the functionality of the computer itself and therefore on the interoperability of the system's components[7].

These requirements can be fullfilled by computer operating systems. Applications software on the other hand does not come under the term as this kind of software does not have a direct influence on the system control. Examples for software with such a technical character is

[6] The same stipulation is to be found for instance in sec. 1 (2) (c) of the British Patents Act from 1977 and in sec. 1 (2) of the German Patents Act from 1981.

[7] BGH GRUR 1992, 33 – "Seitenpuffer"

software that improves the performance of the hardware components of a data processing equipment by enabling a greater storing capacity or by accelerating the processing speed.

From the information given about TRIP the "multimedia search engine", the "reservation and information system, the "Interfaces" and the "Electronic commerce component" do not seem to have such an influence on a computer operating system. They focus on promoting and connecting a new reservation and booking system. The TRIP software has no effect on the outer, physical world but only on the user´s imagination. It neither has an impact on the performance of the hardware components. As an application and database software it lacks any technical character. Thus, the TRIP software, or more exactly, the underlying principle is in our view not patentable.

2.3.2 Would we be liable if we did not register a patent ?

Underlying the result of question 1, that TRIP as a whole or in parts cannot be patented, liability can not be assumed.

2.3.3 Does a patent already exist that specifies a TRIP type system or elements used within the TRIP system ?

This question can only be answered sufficiently if a so called "search of novelty" has been performed by the European Patent Office (EPO) or a national patent office. This means that the EPO searches in specialist journals, data bases and other means at its disposal whether there already exists such a product or not. However, the search and the examination of the material criteria (Does the product fulfil the legal prerequisites of a product which can be patented?) will only be performed after the formal criteria (e.g. Was the application form filled in correctly ? Has the fee been paid ?) are fulfilled. The applicant has got 7 years from the time of completion of the formal criteria to decide whether he wants the EPO to start the examination of the material criteria and the novelty search. If he decides so, another fee has to be paid. Within this 7 year period, the product acquires some minor protection which is limited to the payment of an appropriate amount of compensation.

2.3.4 What options do we have if a patent does exist - i.e. fight it or pay royalties ?

Underlying again the result of question 1, that TRIP as a whole or in parts cannot be patented, it is very unlikely for the same reasons that a similar system exists for which patent protection has been granted. Therefore this conflict will possibly not arise.

However, if such a system should exist Art. 99, 100 EPC offers the possibility for any person to give notice to the EPO of opposition to the European patent granted within nine months from the publication of the mention of the granted European patent.

Supposed that system has been patent protected in accordance with the formal and material legal criteria of the EPC (and Art. 99, 100) no further actions but paying royalties can be taken.

2.4 Protection of the TRIP system and software by copyright law (No. 22, 25, 26)

We decided to deal with question No. 22, 25 and 26 all in one because they are strongly connected with each other.

2.4.1 Which elements of TRIP can be protected by copyright law?

2.4.1.1 The TRIP system as such

The TRIP system as such, i.e. the underlying principle of TRIP, cannot be protected by copyright for it is a mere idea. It is a basic principle of copyright law that ideas are free. The author cannot prohibit its use by other persons. Thus, from the point of view of copyright law, competitors are free to copy the idea of TRIP and to create a similar reservation and booking system. However, such a copy of the idea of TRIP might, under certain conditions, be deemed as unfair competition and therefore be illicite.

2.4.1.2 Information contained in the TRIP system

The same principle applies to the information contained in TRIP and in its documents and web sites. The information as such does only constitute an idea and therefore is not protectable. Only the concrete form of the idea, such as a written text or a picture may be protected.

2.4.1.3 The TRIP software

The TRIP software is protected by copyright law when it is original in the sense that it is the author's own intellectual creation. The software protection does not depend on any qualitative criterion. The TRIP software is very likely to fulfill the originality prerequsite. The ideas and principles that underlie the TRIP computer programs, including those which underlie its interfaces, are not protected by copyright.

2.4.1.4 Elements on the TRIP Web pages

The single elements of the TRIP web pages might be subject to copyright. Under copyright law literary works, such as writings and speeches, musical works , artistic works such as architectural works and works of applied art, photographic works, cinematographic works as well as illustrations of a scientific or technical nature, such as drawings, plans, maps, sketches, tables and three-dimensional representations can be protected.

In the civil law countries (EU member states with the exception of United Kingdom and Ireland) a substantive condition for a copyright protection is the achievement of a certain necessary level of creativity. This condition for example is drawn from sec. 2 para. 2 German Copyright Act which states that only "personal intellectual creations" are works within the meaning of the German Copyright Act. In case the necessary level of creativity is not achieved, only a protection as a related right or neighbouring right is afforded to accomplishments which approach the creation of a work or which are closely related to the performance of a work (regulated e.g. in sec. 70 to 87 German Copyright Act, for instance the protection of certain editions, photographs, performers, producers of sound records and broadcasting organisations). The distinction between copyright and neighbouring rights might be crucial as neighbouring rights afford a limited protection in as far as the duration of neighbouring rights ranges from twenty five years (scientific editions, posthumous works, organisation of a performance) to fifty years (photographs, performers, producers of sound records, broadcasting organisation) while copyright expires seventy years after the author's death (e.g. sec. 64 German Copyright Act). Similar distinctions are to be found in all member states after the implementation of the Council Directive of 29 October 1993 harmonising the term of protection of copyright and certain related rights[8].

[8] Dir 93/98/EEC; OJ L 290/9. The duration of copyright in a literary, artistic, cinematographic or audiovisual work and the duration of photograph protection is set to seventy years after the death of the author or principal director, arts. 1, 2 and 6. The rights of performers expire after fifty years as well as the rights of producers of phonograms, producers of the first fixation of a film and broadcasting organisations, art. 3. The rights in previously unpublished works expire after 25 years, art. 4, the maximum term of protection of critical and scientific publication is set to thirty years, art. 5.

Therefore, a work has to be personal, show a minimal intellectual content and achieve the level of creativity mentioned above. The element "personal" excludes automatically generated documents (for instance a hyperlinklist automatically generated by webcrawler). There is no general definition of the necessary level of creation. German courts decide on a case to case basis if an accomplishment achieves this level. The distinction between a utility work not protected by copyright law and copyrightable applied art for example is drawn by a comparison of the accomplishment with the abilities of an average designer: only if the ability of an average designer is clearly exceeded, the accomplishment is considered to be copyrightable applied art.

If the single element on the TRIP Web site is not protected under copyright it might be protected under related rights. Next to a protection of photographs (which are not photographic works and thus protected by copyright law)[9], the protection of the performer (for example in case of a classical concert videotaped and uploaded as .avi-file to the web)[10], and the protection of the producer of sound records[11] especially a protection as a databank comes into mind. The duration of protection under related rights is often shorter than the protection of works but otherwise the protection under related rights is comparable to that of a copyrightable work.

2.4.1.5 Especially: databases on the TRIP Web site

The databases used within the TRIP system can be protected by copyright law if they amount to so-called database works. This copyright protection requires that the database has a creative character. According to art. 1 para. 2 EC Database Directive[12], whose provisions had to be implemented in national legislation by 1 January 1998 according to art. 16 para. 1[13], a databank is defined as a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. A copyright protection applies to databases which, by reason of the selection or arrangement of their contents, constitute the author's own intellectual creation.

Additionally, the EC Database Directive provides for a *sui generis* right of the maker of a database which shows that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilisation of the whole or of a substantial part evaluated qualitatively and/or quantitatively, of the contents of that database, art. 7 para. 1 EC Database Directive.

---

[9] Sec. 72 German Copyright Act.

[10] Sec. 73 et seq. German Copyright Act.

[11] Sec. 85 German Copyright Act.

[12] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77 p. 20. URL: http://www2.echo.lu/legal/en/ipr/database/database.html.

[13] As of now, the directive has been implemented in sec. 4 para. 2 (definition of a databankwork), sec. 53 para. 5, 55a, 63 (exemption provisions) and sec. 87a et seq. (sui generis protection of databases) German Copyright Act.

In case they do not fulfill this requirement the database can be protected by a so-called sui-generis right which gives the rightholder a less strong position. Under sec. 87a et seq. German Copyright Act and the respective provisions of the other EU member states a databank does not need to be an author's own personal creation. It is protected if its maker has made a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilisation of the whole or of a substantial part of the contents of that database. Arguments for a substantial investment may be labour force, money, or time invested in creating the database.

2.4.1.6 The TRIP Web pages as a whole

Beneath a copyright protection for single elements on the TRIP Web pages like text, images, sound, videos and databases the pages as a whole can be subject to copyright. Here, a protection as a computer program could be imagined. A computer program is protected if it is original in the sense that it is the author's own intellectual creation.

A WebPage could be considered a computer program if HTML, VRML, XML, Java or Javascript, or other applications with which a WebPage can be designed, are programming languages. "Program" is usually defined either as a complete structured sequence of program statements directing a computer to implement an algorithm or all software programming necessary to solve a problem. The most commonly used application to design a WebPage, HTML, however, is not foreseen to implement any algorithms. In spite of its mechanisms for style sheets, scripting, frames, embedding objects, improved support for right to left and mixed direction text, tables, and enhancements to forms, HTML is basically still a simple text based generic mark-up language or page description language. The term thus officially used for HTML is "publishing language". The same applies to the formatting languages VRML, a file format for describing interactive 3D objects and worlds and XML which describes a class of data objects called XML documents and partially describes the behaviour of computer programs which process XML documents but which are not computer programs themselves. As formatting elements or graphical descriptions HTML, VRML and XML elements can be protected only as layout (where the layout exceeds a certain necessary level of creativity and can be considered to be applied art according to sec. 1 para. 1 no. 4 German Copyright Act), or together with the literary or other work.

Scripting languages like Java or ECMAScript, however, are specifically designed to implement algorithms and solve problems. These languages are not only used to describe formatting which then is processed by an addressed browser, but functionally used to solve algorithmic problems within the WebPage. As such, however, a WebPage programmed in Java or another scripting languages can theoretically fall under the provisions of sec. 69a German Copyright Act with the implications mentioned above. As sec. 69a para. 2 German Copyright Act protects the expression in any form of a computer program, even the design of a WebPage

might be protected under sec. 69a et seq. German Copyright Act if the design is programmed in a scripting language.

Here, the difficulty arises to prove that the computer program has originally been achieved by the person who claims authorship. Especially with the relatively short scripting used in Web-Pages today and easy access to the source code as the scripts are usually not compiled, this will be one of the major difficulties TRIP would have to tackle when claiming a copyright infringement in or out of court.

2.4.2 Formal conditions of copyright protection

Copyright originates with the creation of the work. It does not depend on a formal condition suc as registration or payment of a fee. The use of the copyright symbol is not necessary. Nevertheless, it can be useful from a practical point of view to stress the subsistence of copyright by a copyright notice. In the UK literary works, e.g. texts or computer programs, must be recorded in any form (sec. 3 CDPA). In the context of TRIP this prerequsite does not play an important role. In the civil law countries there are no formal requirements to be met. The protection of neighbouring rights in some member states depends on formal conditions such as fixation. In some member states, e.g. in Sweden and in Spain, it is possible to register a work voluntarily.

2.4.3 Who is the copyright holder? Who owns copyright in a Web page? (No. 22, 27)

In countries following the "intellectual creation principle", i.e. in Austria, Belgium, Denmark, France, Finland, Germany, Greece, Italy, Luxembourg, Norway, Portugal, Spain and Sweden the copyright generally is bound to the author of the work.If TRIP has engaged a designer for the creation of its web site or charged an employee with this task, not TRIP or its partners but the designer/employee owns the copyright in the pages. The person who created the site only may grant contractual exploitation rights to the employer, for instance exclusive rights of utilization.

In Ireland, Great Britain and the Netherlands the employer may be the original copyrightholder, even if this is a legal entity. According to Irish copyright law the employer is entitled to the copyright in the work which is made in the course of the author's employment under a contract of service or apprenticeship. Similarly, in the Netherlands, employers are entitled to the copyright in works created by employees whose tasks include the creation of such works.

2.4.4 Do we need to ensure that any contracts awarded to designers for creation of new web sites /pages include a clause obliging him/her to assign copyright to TRIP?

As we have seen in the answer to question 22, copyright generally is bound to the author of the work. In the countries that apply the personal creation pricnciple is not possible to make the designer or employee assigncopyright to TRIP. However, the author may exclude himself from all rights of utilization. TRIP could try to implement such a clause in its contracts with Web designers.

In Ireland and the United Kingdom, the copyright as a whole may be transferred to another (natural or legal) person by statute or contract. Insofar, TRIP should draft a contract with the designer or with the employee who creates the web pages that transfers the copyright in the pages.

2.5 Hyperlinks (No. 28)

TRIP might use on its Web site hyperlinks to other sites containing copyrightable material. The question arises whether any exploitation right or moral right of the author of the targeted site is concerned. Until today there is no clear and uniform jurisdiction on this topic. Therefore, we can not provide TRIP with reliable instructions for the use of hyperlinks. However, we will list up those types of links that might be deemed as a copyright infringement.

A normal hyperlink should not lead to any copyright problem. A hyperlink is no reproduction of the targeted web page. It only enables the user to navigate from one page to another. It informs the browser where to find a certain document, but is does not contain the document itself. As the user has to go to the targeted site himself by clicking onto the link, a hyperlink is comparable to a footnote but not to a copy. Further on, a hyperlink is not to be regarded as a kind of communicating the targeted site to the public. It is not the link that provides the user with the protected material, but the user himself who requests it -by the help of the link.

In case of a link that bypasses the homepage of the targeted site (so-called deep link)the situation is more difficult. The link might be deemed an unfair competition act. In the event of a link to protected material that by-passes an information on copyright restrictions the provider of the link could facilitate a copyright infringement by the user and, thus, might be held liable for contributory infringement.

On the TRIP web site pictures or other objects might be displayed by use of links which make the web document display an image that is not stored within this document but elsewhere on the Internet (so-called in-line links). The visitor of the TRIP site will not even recognise that

the picture originates from a different site. This kind of using third author´s material would, in our view, be an unauthorised reproduction, though, from a technical point of view, the link only tells the user´s browser where to find a certain document. But for the user the situation is the same as if the picture were part of the page that contains the link.

Beneath the reproduction right the right of communication to the public is concerned. Under certain circumstances also a moral right, such as the right to recognition of the authorship and the right to respect for the integrity of one´s work may be infringed. Inline links could also be deemed a trademark infringement or an unfair competition act.

As regards gopher there are no different problems.

2.6 Caching and other ephemeral storing as a copyright infringement? (No. 29)

The storage of digitised data needs either to be authorised by the author´s expressed or tacit consentment or by an exemption provision such as the private use or fair use rule.[14] Thus, the question arises if the more or less transient storage of the material such as the caching or the storage in the Random Access Memory (RAM) amounts also to an act that is restricted by copyright law. The British CDPA is the only act which stipulates expressly that copying includes the making of copies which are transient or incidental to another use of the work (Art. 17 (6) CDPA). Thus, in the UK the ephemeral storage on the RAM is covered by the reproduction right.

In all other Member States there is still a substantial debate on this question. In our opinion caching and other more or less ephemeral reproductions, such as swap file storage or even the mere screen display, are not to be deemed an act restricted by copyright law. These "reproductions" only have a technical but not an economical significance. They are not meant to make possible a separate economic use.

However, if one regards caching or RAM storage as a reproduction act, there will often be a tacit authorisation (implied licence). The right-holder who puts his works into the net knows and wants that these works are visited by users, to the degree that he does not install any technical access control. This does not apply to those countries where the reproduction right can only be licensed or transferred by a contract in written form. If the content has been put into

[14] See Sec. 15 (1) Austrian Copyright Act; Art. 1 Sec. 1 Belgian Copyright Act; Sec. 2 (1) Danish Copyright Act; Art. 2 (1) Finish Copyright Act; Art. 122-3 French Copyright Act; Sec. 16 (1) German Copyright Act; Art.3 Greek Copyright Act; Sec. 8 (6) (a) Irish Copyright Act; Art. 13 Italian Copyright Act; Art. 3 Luxembourg Copyright Act; Sec. 2 (1) Norwegian Copyright Act; Art. 68 (2) (d) Potuguese Copyright Act; Art. 18 Spanish Copyright Act; Art. 2 (1) Swedish Copyright Act; Art. 17 United Kingdom Copyright, Designs and Patent Act.

the Net without the author's consentment the screen display is, in most cases, allowed because of the private use exemption.

2.7 Liability for copyright infringement (No. 30)

This question will be answered in the second part of the assistance document.

3 Data protection Issue (answer to question 17):

Any data taken from TRIP Agents or their customers is subject to the Data Protection act in the UK. What relevant legislation exists in other partner countries?)

In principle, national data protection laws existing in the different Member states of the European Union must be modified in order to comply with the EU directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

At first one must determine whether or not data protection laws will apply in general. This will depend on whether or not personal data is being processed. Personal data, according to article 2.a of the EU directive covers any personal data relating to an identified or identifiable natural person". A natural person can either be directly identified by reference to his name or an identification number for example, or can be indirectly identified by reference to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Some Member states have gone further in that they extend the scope of data protection laws to legal persons (see Italian data protection law of 1997, article 1.1.1.).

If personal data is being processed, then one must determine which national data protection law applies. According to the data protection directive, this will depend on the place of establishment of the data controller. This is a question of international private law.

ANNEX 7: Assistance to TRIP : Second set of answers

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

Consumer Protection, Liability Issues and International Private Law Issues Relating to TRIP

Rosa Julia-Barcelo (CRID), Anne Salaun (CRID), Peter Lenda and Morten Foss (NRCCL)

CONTENT

LIABILITY ISSUES (Rosa JULIA BARCELO)

INTRODUCTION

For the purposes of establishing the liability claims that TRIP Inc could face, this memo is divided into fourth sections:

The first section starts with a description of the project that enables one, in the second section, to discern the functions carried out by TRIP Inc.

The third section, after providing a description of the so-called "on-line intermediary functions", examines the types of liability claims that TRIP.Inc could endure in its function as search engine. In particular, reference is made to extra- contractual liability and contractual liability suits. In addition, several clauses are suggested for inclusion in the contracts between TRIP actors.

The fourth section assesses the liability claims that TRIP.Inc could face derived from its function as electronic agent.

The four sections aim at providing answers to the questions that were raised by TRIP.Inc. regarding liability. In addition, they seek to present a general overview of the liability issues that TRIP.Inc. could face as a result of its activity as search engine provider and electronic agent. This memorandum may not cover every liability issue that might be faced by TRIP.Inc, and I will be happy to answering further questions in this area.

I.- SUMMARY OF THE PROJECT

The TRIP system is a search engine owned by TRIP.Inc that, upon request of information, in return provides a list of suitable products under set contractual terms or alterna-

tives. In order to do so, the engine is connected to various databases of information kept by suppliers (referred to as TRIP operators).

The TRIP system is targeted, inter alia, to travel agents and hotels. In particular, those actors will have access to the search engine via the Internet with a browser that will have been licensed to them by TRIP. Inc.

II.- CLASSFYING THE ROLES CARRIED OUT BY TRIP.INC.

The first issue to be clarified is defining what are the *specific roles* carried out by TRIP.Inc. This will permit us to assess the possible liability actions that TRIP.Inc could face.

In principle, from the above description, it seems that the functions carried out by TRIP.Inc. are the following: First, an on-line intermediary function consisting in locating information, and second, an electronic agent function consisting in entering contracts on behalf of suppliers. Both roles will be discussed below.

II.1.- Defining on-line intermediary roles and their application to Trip. Inc.

From the description of the TRIP project, it appears that it carries out on-line intermediary functions. To the extent that the liability of on-line intermediaries has been addressed by the Proposal for a Directive on certain legal aspects of electronic commerce, on this basis, we could establish the obligations that TRIP should carry out to avoid liability.

On line intermediaries

By on-line intermediaries should be understood as being those actors who do not take part in the creation or selection of information to be disseminated. Instead, on-line intermediaries play various roles in the on-line dissemination of information provided by so-called "content providers".

In particular, the different functional roles that can be carried out by on-line intermediaries are basically the following:

• Network operator: providing the facilities for the transmission of data such as cables, routers and switches.

• Access provider: providing access to the Internet. Users connect to the Internet through their access provider's server. Commonly, an access provider also provides an e-mail account.

• Host service provider: providing a server upon which it rents space to users to host content, for instance a web page, which can incorporate all kinds of material (such as software, text, graphics, and sound).

• Bulletin board operators, news groups and chat room operators: services providing space for users to read information sent by other users and to post their own messages. Usually, they are devoted to specific topics. There are two types of newsgroups: moderated and unmoderated. The chat room allows direct communication in real time.

• Information location tool providers: providing tools to Internet users for finding web sites where information they seek is located. There are two types of search engines, namely automated search engines and search engines that rely upon human beings to review and catalogue web sites.

Functions carried out by TRIP Inc.

As described in the first section, TRIP Inc provides the clients with a browser that enables a connection with a search engine that provides access to information supplied by TRIP operators.

From the description of the TRIP functions, in principle it can be established that it does not carry out on-line intermediary functions such as providing facilities for the transmission of data (cables, routers and switches), access to Internet, or renting server space to users to host content.

However, there appears to be a substantial similarity between TRIP.Inc's search engine function and the information location tools function. Indeed, the search engine, as does an information location tool provider, reviews the web sites where the suppliers have the information about their products, catalogues the sites, and then, if the end-user wishes so, provides the tools for contracting the services offered by the suppliers. Therefore, it appears that the search engine accomplishes two functions: First, a *search engine* function and, second, an *electronic agent* function.

II.2.- Defining electronic agent functions and their application to TRIP.Inc.

Electronic agents in general are programmed to search for (on behalf of a potential purchaser) or make available (on behalf of a potential licensor) particular types of information under set contractual terms or alternatives. The reduced transactional costs are significant, permitting broad comparative shopping.

As described earlier, TRIP.Inc. provides not only a search engine that allows access to information, upon request, but also permits the end-user to enter contracts with the supplier for the provision of the services described in the information supplied.

Nowadays, in Europe, the law does not regulate the liability of electronic agents. Therefore, the activities of electronic agents raises some doubts about the legal regime that will apply. For example, to what extent will the person who uses the agent be responsible for the action of the agent?. A solution for the lack of specific law consists in applying by analogy traditional agency law. For example, agency law could be used by courts to establish whether in a particular situation, the contractual message sent by the agent is attributable to the person used the agent.

However, because of the uncertainty of the law that could be applied in case of law-suit, it will be wise for the trading parties (TRIP.Inc with suppliers and TRIP Inc with travel agents or hotels) to specify by contract a legal regime.

In the next sections, I will endeavour to assess liability actions in tort that TRIP.Inc could face as a search engine and as an electronic agent. In addition, I will provide contractual clauses that TRIP.Inc should include for the purpose of limiting or excluding its contractual liability.

III.- ASSESSING POSSIBLE LIABILITY ACTIONS AGAINST TRIP.INC IN LIGHT OF ITS FUNCTION AS SEARCH ENGINE

The first distinction should be drawn between liability actions based on tort (referred to also as extra-contractual liability) and liability actions based on contract. The first arises when a law or a right has been violated. Member States require fault for damages to be granted, which means that liability is granted when the damages have been produced because of negligence (or some other standard of fault) of the actor. Contractual liability arises upon breach of contractual obligations.

III.1.- Extra-contractual liability actions

TRIP. Inc could face extra-contractual liability actions brought by third parties for providing access to certain sites containing infringing or illegal content. The grounds for this action would be similar to those alleged against site operators for having *linked* a document with another document containing infringing or illegal material. Indeed, hyperlinks are points in web documents through which users may access directly to other documents, allowing the users to search for information easily. A type of hyperlink referred as "in-line link" is a pointer to a document, image , audio or the like somewhere on the web contained in another's web page which pulls in the image into the current document for display.

There have been several lawsuits brought against owners of sites that linked a document with another document containing illegal information[1]. So far, to my knowledge there are no lawsuits against search engines. However, given the similarity of the functions carried out by search engines and those of others involved in "linking" it is foreseeable for them to occur.

As far as the law that is infringed is concerned, it is possible to distinguish between several bodies of law: For example, a third party could maintain that the search engine has violated its intellectual property rights by providing access to information without permission of the owner of such rights. Other rights or laws that could be alleged to have been violated are, inter alia, the following ones: illegal and harmful content, private and defamatory material (such as pictures taken in intimate situations), trade secrets, and misrepresentation, i.e., when false or incorrect information provided by someone causes damage to a third party.

Given the nature of the information to which TRIP.Inc provides access, it is unlikely for this information to be illegal, harmful or defamatory. However, it is conceivable that TRIP.Inc could face liability actions for violation of intellectual property rights and also for

[1] - See for example Shetland Times Ltd. V. Wills, Scot. Sess. Cas., (10/24/96), settled Nov. 11, 1.997; Ticketmaster Corp. V Microsoft Corp., No. 97-3055 (CD. Cal., complaint filed Apr. 28, 1997).

misrepresentation. For example, if Trip operators render wrongful information about prices and airline schedules, a third party that has suffered damage as a result of such wrongful information could claim damages.

Answers provided by the Proposal for a Directive on certain legal aspects of electronic commerce

The Proposal for a Directive has not addressed the on-line function of search engines. Therefore, in order to ascertain which liability regime will apply to search engines, the grounds may be found in the case law decisions on linking. Unfortunately, existing case law involving linking has been settled by parties before that courts could address the issue.

It should be noted that the liability for search engines is addressed in the U.S. Digital Millenium Copyright Act of 1998. Specifically, this Act establishes both an actual and constructive notice standard to those who provide information location tools. The legislative history provides that constructive knowledge of infringement should not be imputed to directory providers (search engine providers) simply because the provider viewed an infringing site during the course of assembling the directory.

Actions that could be taken by TRIP. Inc. to prevent tort liability

TRIP.Inc. cannot prevent the above actions (tort liability) from being filed and furthermore, cannot exclude its extra contractual liability. However, TRIP Inc. can take several steps anticipating these actions and establish remedies. In particular, the following steps could be undertaken:

First, in the contractual agreements signed between TRIP. Inc and the suppliers (referred to as TRIP information providers) for the purposes of establishing the obligations of both, search engine and information provider, TRIP Inc. should try to include a clause establishing that the information provider is responsible for the information it itself provides. In particular, the following contractual clauses should be included:

(a) The TRIP information provider has the obligation to clear the copyright of the material that is sent to the search engine (such as pictures accompanying information about the tickets) and trademarks. If the information provider fails to fulfil this obligation and TRIP.Inc is sued, the information provider will pay the damages necessary to restore TRIP.Inc to its position (i.e., idemnify TRIP.Inc.).

(b) If TRIP.Inc. is condemned to pay damages to third parties because of complaints granted by the court on the basis of the information received from the information provider (for example, defamatory or misleading information), the information provider will have to restore TRIP.Inc to its position (i.e position (i.e., indemnify it for any damages awards granted against it with respect to any information provided by the TRIP. information provider).

Second, it should obtain an insurance policy to insure against tort liability actions. For example the so-called "comprehensive general liability insurance" includes coverage for advertising, and offences like defamation, copyright infringement. The "E&O Insurance" covers losses and liabilities steaming from errors and omissions of computer services (for example, this insurance is supposed to apply to the year 2000 bug). Another interesting insurance is the "advertising and publishing liability insurance". It ensures against claims from the policyholder's advertising activities, including demands for violation of privacy, defamation, libel, intellectual property rights, etc. In any event, the insurance policy should be read carefully to see what it covers.

III.2.- Contractual liability actions

The grounds for this action will be found in a breach of the contractual obligations that bind TRIP. Inc. as a result of a contract with the supplier. For example, the supplier might

have licensed to TRIP.Inc the use of its trademark for a particular purpose and in certain circumstances. If TRIP.Inc. violates these provisions, the supplier can file a complaint against TRIP.Inc.

In principle, to the extent that TRIP.Inc fulfils its contractual obligations, these type of liability actions should not constitute an issue. As we will further analyse, these type of liability actions are more likely to occur not because of breach of contract regarding the use of information (such as copyright, patents, etc.) but as a result of a breakdown of the search engine. In addition, it should be noted that insurance companies are designing new insurance policies tailored to the new Internet businesses practices.

IV.- ASSESSING POSSIBLE LIABILITY ACTIONS AGAINST TRIP.INC. IN LIGHT OF ITS FUNCTION AS ELECTRONIC AGENT

As described earlier, TRIP.Inc. not only provides a search engine function but also permits the end-user *to enter a contract* for the provision of the services provided by the supplier. This function is usually referred to as "electronic agent".

This function resembles the role carried out by traditional "agents". Agency is regulated by Directive 86/653, 18 of December 1986, which has been implemented in all Member States. In particular, and according to the Directive, an agency contract establishes the authority of the agent to negotiate and enter contracts on behalf of the principal.

As mentioned earlier, as far as Trip.Inc's function as a search engine is concerned, in principle, it appears that TRIP. Inc could face both tort and contractual liability actions. However, given the nature of the function carried out by the electronic agent, entering contracts on behalf of the principal, it seems more likely that the person who will file a lawsuit against the agent will be the one who uses the services of the agent. For example, the information pro-

vider or the person who enters the contract (the hotel or travel agency) on behalf of the end user. Therefore, to the extent that there will be a contractual relationship among these actors, it seems likely for the actors to file lawsuits based on contractual actions. Therefore, let us to analyse the contractual claims.

.

IV. 1.- Contractual liability actions

Before, dealing with contractual liability actions, it is essential to enumerate and describe the contracts that need to be entered by TRIP.Inc. Afterwards, I will endeavour to provide exemplary contractual clauses that TRIP.Inc should include in its contractual agreements.

In particular, Trip.Inc has to enter the following contracts: First, a contract with Trip information providers and, second, it has to enter a license agreement with the travel agency or hotel. Both contracts are analysed below.

In addition, once the electronic agent is running, it will enter thousands of contracts on behalf of the information suppliers with the hotels and travel agencies (who, at the same time will act on behalf of end users).

Contract between TRIP.Inc and TRIP information providers

This contract will establish the obligations of both the information providers and TRIP.Inc. Concerning the obligations of the information providers, TRIP.Inc should try to include the following clauses:

(a) The information provider has the obligation provide to the TRIP.Inc. the information it has engaged to provide. If it fails to perform this obligation and TRIP.Inc was sued, the information provider will pay the damages to restore TRIP.Inc. to its position.

(b) The information provider has to fulfil the obligation it has engaged in when providing information about the services it supplies. If the service was not performed and TRIP.Inc was sued, the information provider will pay the damages to restore TRIP.Inc to its position. For example, if the electronic agent enters contracts with hotels for the provision of certain "tours" that were offered by the information providers, if they decide not to perform the "tours", and TRIP. Inc. is sued and has to pay damages, the information providers have to restore TRIP.Inc. to its initial position.

In the contractual agreements, TRIP.Inc should try to include the following:

The information providers accept that TRIP.Inc. will enter contracts (using an electronic agent) for the provision of services on TRIP.Inc behalf; accordingly, they will be responsible for the contracts entered into by TRIP.Inc.

As far as limitations and exclusions of liability, TRIP.Inc should consider the adoption of the following clauses:

First, disclaimer of warranties.- TRIP.Inc should establish in the contract that no software can be made bug-free and should try to exclude warranties of fitness .

Second, disclaimer of ancillary representations.- TRIP.Inc should include a clause having the effect of excluding reliance by the information providers on warranties or representations not contained in the contract.

In addition, it could happen that as a result of a failure in the system, TRIP.Inc provides non-accurate information upon which the travel agency or hotel relies. For example, it could be conceived a situation where the electronic agent provides by mistake some information offering very cheap rates for a certain destination, and hotels and travel agencies book this flight on the basis of the cheap price. If the information supplier does not want to provide the flight at that price --because he never wanted to make such offer-- the travel agency may

seek damages from both the information provider and TRIP.Inc. As far as the information provider is concerned, if it is condemned either to pay damages or stick to the contract (i.e., the contract entered by the agent on its behalf is regarded as valid[2]), the information provider may wish to recover his losses from TRIP.Inc. In this regard, TRIP.Inc should establish that it will be responsible to the information supplier at the most for direct loss but not consequential damages. Alternatively, TRIP may introduce monetary caps on its liability.

Besides the contractual agreement solutions, TRIP.Inc should consider to obtain insurance to cover such losses. For example, the "property and business-interruption insurance" covers losses such as interruption or suspension of the service due to failures of the technology or congestion of the networks. Another interesting policy insurance is the "fidelity insurance and bonds" which will protect against losses arising from fraud and theft by employees and non-employees.

Contract between TRIP.Inc and travel agents/hotels

TRIP.Inc should enter a license agreement with the travel agencies and hotels. In this agreement it should be establish the obligation of TRIP. Inc to provide a browser and a connection to the search engine that performs agency functions with reasonable skill and care. Concerning liability disclaimers to be included in this contract, TRIP.Inc should consider the adoption of the following ones:

[2] - It falls outside the scope of this memo to assess weather an error will entail that the contract is void. In particular, by applying general rules of mistakes, if the following requirements are met, the contract will be voidable: (1) there is a mistake of one party at the time of the contract, made as to a basic assumption on which the contract is made; (2) the sender is not at fault in initiating the erroneous message, (3) the recipient should have had reason to know that there was an error or mistake.

First, disclaimer of warranties and limitation of damages.- TRIP.Inc should establish in the contract that no software can be made bug-free and should try to exclude warranties of fitness. In addition, it could be established that the person who owns the software shall not be liable to the person using the software for any damage caused to them or third parties in connection with the software. For example, it could be included the following liability disclaimer: TRIP.Inc. and/its information provider make no representations about the suitability of the information, services and the software for any purpose. All such information, services and software are provided "as is" without warranty of any kind. TRIP.Inc. and/or its information providers disclaim all warranties and conditions with regard to this information, services and software, including all implied warranties and conditions of merchantability, fitness for a particular purpose. In any event should TRIP.Inc. be liable for any direct, indirect, punitive , incidental or consequential damages arising out or in any way connected with the use of the TRIP. system or with the delay or inability to use it. It should be noticed that limitations upon warranties are some times not enforceable. I have not investigated weather this particular limitation would be enforceable in those countries where TRIP.Inc. will license the browser.

Second, disclaimer of ancillary representations.- TRIP.Inc should include a clause having the effect of excluding reliance by the travel agents on warranties or representations not contained in the license agreement.

In addition, it should be taken into account that in the contract between TRIP.Inc and the travel agencies or hotels, --probably, by request of the information providers--, it will be included an obligation of using technological means to ensure the authenticity and integrity of the electronic messages (often referred as authentication procedures) such as digital signatures and certificates. In particular, contractual messages such as the offers and acceptances. This paper does not deal with this issue; however, because the failure to carry out this function may entail liability, it is important to include a clause establishing who bears the risk and its limits.

In this regard, it could be established that failure to carry out this "security" obligation by a contracting party will obligate this party to pay any resulting damages. For example, this could happen if TRIP.Inc fails to check the validity of a hotel's digital certificate that was revoked by the hotel upon discovery of its compromise. Then, TRIP. Inc enters a contract

with a "fraudulent hotel" purporting to be the real one. According to the above provision, the real hotel will not be responsible for this order, but the information provider who acted by using the electronic agent will be responsible. Of course, in the contract between TRIP.Inc. and the information provider, it should be established that TRIP.Inc will reimburse the information provider for the damages it has suffered as a result of its failure to use the appropriate technical means.

CONSUMER PROTECTION (Anne SALAUN)

1. Relation between the TRIP Project and individual consumers

Since the TRIP project is aimed at targeting travel agents and not directly individual consumers, consumer protection rules will not apply. Indeed, consumers will only take advantage of the system in place through a travel agent acting as an intermediary. Therefore, the provisions protecting consumers with regard to distance contracts are not relevant. Likewise, the question as to the language in which the information must be presented is not a crucial point since the legislation in this matter aims mainly at protecting individual consumers.

1.1. Distance Contracts Directive

With regard to the contracts concluded at the occasion of the TRIP system, the consumer is not directly involved: it appears indeed that the contract will be concluded by the travel agent - on behalf of the consumer - and thus the consumer will not be a party of the contract. Consequently, the Directive concerning the protection of consumers in respect of distance contracts[3] will not apply as the distance contract is defined as "any contract concerning goods or services concluded between a supplier and a *consumer* under an organised distance sales or service-provision scheme run by the supplier (...)"[4]. A consumer is heard in the European consumer protection legislation as a natural person who is acting for purposes which are outside his trade, business or profession.

[3] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997, OJEC L 144 p.19.

[4] Article 2 (1) of the Directive.

1.2. Language requirements

As far as the language in which the information is presented is concerned, the same remark applies since consumers are not the direct target of the project. We do not find anyway any rule at the European level imposing to provide an information in the consumer's language: the sole requirement is that the information is provided in "a clear and comprehensible manner" (article 4 of the Distance Contracts Directive). This rule concerns the prior information presented by the supplier before the conclusion of any distance contract.

However, some national legislation do impose an obligation to inform the consumer in his own language (it is the case for instance with the French legislation) but this requirement is only applicable in a business-to-consumer context, not a business-to-business one.

2. The TRIP Project and advertising requirements

Nevertheless, consumer protection requirements are not fully excluded from the TRIP Project: indeed, some of the consumer protection requirements have a broader scope of application. It is the case for the rules set forth in the field of advertising – both misleading and comparative – where the purpose is to "protect consumers, persons carrying a trade or business or practising a craft profession, and the interests of the public in general against misleading advertising (...) and to lay down the conditions under which comparative advertising is permitted"[5].

[5] Article 1 of Directive 97/77/EC of the European Parliament and of the Council of 6 October 1997 amending Directive 84/450/EC concerning misleading advertising so as to include comparative advertising. http://www.europa.eu.int/comm/dg24/policy/developments/comp_adve/comp_adve02_en.html

Advertising produces general effects on the functioning of the internal market, it is thus logical that the protection is not limited to individual consumers since competitors and the market more generally can suffer from a misleading advertising or from a comparison that do not comply with the rules set forth in the Directive. The TRIP Project will therefore have to comply with advertising requirements.

2.1. Advertising requirements at the European level

An advertising Directive was first adopted in 1984 concerning exclusively misleading advertising. This Directive had to be implemented by the Member States by 1st October 1986 at the latest. Then the European Commission expressed the wish to go further in the field of advertising by allowing comparative advertising under strict conditions. A new Directive adopted on 16 October 1997 is intended to amend the misleading advertising Directive. This Directive has to be implemented by Member States at the latest 30 months after its publication in the Official Journal of the European Communities, so by the 23 April 2000.

It is important to mention that those legislation have a general scope of application and do apply to any form of advertising, be it on the Internet or not.

The TRIP Project will have to comply with the legislation in force at the European level with regard to advertising, namely the Misleading Advertising Directive and the Comparative Advertising Directive. Moreover, account should be taken of the recent draft Directive on certain legal aspects of electronic commerce[6] and on its provisions related to unsolicited commercial communications.

2.1.1. Misleading advertising: Directive of 10 September 1984[7]

Advertising is heard as "the making of a representation in any form in connection with a trade, business craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations". Misleading advertising is defined as "any advertising which in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature,

---

6 Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, 18 November 1998.

7 http://www.europa.eu.int/comm/dg24/policy/developments/misl_adve/misl_adve01_en.html

is likely to affect their economic behaviour or which, for those reasons, injures or is likely to injure a competitor"[8].

In determining whether an advertising is misleading, account should be taken of all its features, and in particular of any information it contains concerning:

a) the characteristics of goods or services, such as their availability, nature, execution, composition, method and date of manufacture or provision, fitness for purpose, uses, quantity, specification, geographical or commercial origin or the results to be expected from their use, or the results and material features of tests or checks carried out on the goods or services;
b) the price or the manner in which the price is calculated, and the conditions on which the goods are supplied or the services provided;
c) the nature, attributes and rights of the advertiser, such as his identity and assets, his qualifications and ownership of industrial, commercial or intellectual property rights or his awards and distinctions.

In the frame of an administrative or judicial control of those provisions, the Directive mentions that the advertiser may be requested to provide evidence as to the accuracy of factual claims in advertising if, taking into account the legitimate interests of the advertiser and any other party to the proceedings, such a requirement appears appropriate on the basis of the circumstances of the particular case. If such evidence is not furnished by the advertiser or deemed insufficient by the court of the administrative authority, the factual claims will be considered inaccurate, opening either a cessation procedure or a prohibition of publication[9].

2.1.2. Comparative advertising: Directive of 6 October 1997

The purpose of this Directive is "to protect consumers, persons carrying on a trade or business or practising a craft or profession and the interests of the public in general against misleading advertising and the unfair consequences thereof and to lay down the conditions under which comparative advertising is permitted". Comparative advertising is heard as "any advertising which explicitly or by implication identifies a competitor or goods or services offered by a competitor"[10].

The conditions for allowing comparative advertising are rather strict as, on the one hand, they are devoted to grant a better information to consumers, but on the other hand they represent the wish to avoid any distortion in competition through any detriment to competitors and adverse effect on consumers' choice. Therefore, the following conditions have to be fulfilled:

---

8 Article 2 § 2 and 3.

9 Depending on whether the advertising is already published or it has not been published but its publication is imminent. See article 4 § 2.

10 Article 1 (2) and (3).

a) the advertising shall not be misleading;
b) the advertising shall compare goods and services meeting the same needs or intended for the same purpose;
c) the advertising shall compare objectively one or more material, relevant, verifiable and representatives features of those goods and services, which may include price;
d) the advertising shall not create confusion in the market place between the advertiser and a competitor or between the advertiser's trade marks, trade names, other distinguishing marks, goods or services and those of a competitor;
e) the advertising shall not discredit or denigrate the trade marks, trade names, other distinguishing marks, goods, services, activities, or circumstances of a competitor;
f) for products with designation of origin, the advertising shall relate in each case to products with the same designation;
g) the advertising shall not take unfair advantage of the reputation of a trade mark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products;
h) the advertising shall not present goods or services as imitations or replicas of goods or services bearing a protected trade mark or trade name.

All these provisions are of strict application, i.e. Member States are not allowed in the implementation process to adopt stricter rules that could possibly lead to the prohibition of comparative advertising.

2.1.3. Proposal for a Directive on Certain Legal Aspects of Electronic Commerce[11]

Commercial communications are defined in the proposal as any form of communication designed to promote, directly or indirectly, goods, services or the image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a liberal profession. It is stated that do not constitute, as such, commercial communications: 1) information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic-mail address, and 2) communications relating to goods, services or the image of the company, organisation or person compiled in an independent manner, in particular without financial consideration.

Article 7 of the Proposal states that Member States should lay down in their legislation that unsolicited commercial communication by electronic mail must be clearly and unequivocally identifiable as such as soon as it is received by the recipient. A recipient is heard as any natural or legal person who, for professional ends or otherwise, uses an information society service.

If partners from the TRIP Project intend to promote their services by contacting directly the travel agents through their e-mail address, they shall be aware of this rule, even though it is

[11] 18 November 1998, http://www.ispo.cec.be/ecommerce/legal.htm

not yet constraining. Any message sent through an e-mail address should therefore clearly identify its commercial nature.

2.2. Advertising requirements at national levels

Member States have their own legislation dealing with advertising, also some extra-regulatory provisions.

Countries in which the Project is active for the time being are the United Kingdom, France, Portugal and Italy.

2.2.1. United Kingdom

2.2.1.1. Legislation

The misleading Directive has been implemented in England in 1988 in a law on 'the control of misleading advertisements regulations'[12]. Advertising is defined in a similar war than the Directive, as well as the misleading character of the advertising, namely an advertising that in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and that, by reason of its deceptive nature, is likely to affect their economic behaviour or, for those reasons, injures or is likely to injure a competitor or the person whose interests the advertisement seeks to promote[13]. Comparative advertising is allowed by the Trade Marks Act of 1994 unless it is detrimental to or unfair to a competitor. Section 10 (6) allows the use of a trade mark for the purpose of identifying goods and services as those of the owner but prohibits such use when:

- it is not in accordance with honest practices in industrial or commercial matters, or
- it takes unfair advantage of or is detrimental to the distinctive character or reputation of the competitor.

2.2.1.2. Code of Practice

A comprehensive Code of Practice has been issued by the independent Advertising Standards Authority[14]. This Code concerns mainly general principles regarding the advertising (the advertising should be legal, decent, honest and truthful), advertisers liability principles, com-

12 Law n° 915 of 23 May 1988.

13 See paragraph 2 (1) and (2).

14 Ninth edition of the Advertising Code and sixth edition of the Sales Promotion Code, February 1995.

parisons, exploitation of goodwill and imitation, the obligation to identify the advertising and the advertiser, etc.

The Code contains also provisions dealing directly with the sale of products (price products, availability of products, guarantees, etc.).

Besides the general provisions, the Codes contain specific provisions aimed at protecting children or specific categories of products like health and beauty products and therapies, alcoholic drinks, cigarette, that do not concern the TRIP Project.

2.2.2. France

The French Consumer Code of 1993, in its Title II 'Commercial Practices' Chapter I 'Regulated Commercial Practices' deals with advertising. General provisions on misleading and comparative advertising are set forth, including control measures and sanctions in case of violation. However, we find no specific provisions devoted to advertising on the Internet.

INTERNATIONAL PRIVATE LAW (Peter LENDA & Morten FOSS)

1. INTRODUCTION

1.1 Introductory remarks

The establishment of a web shop may create several advantages for the retailer. One is the simplification of reaching out to customers located in foreign countries. If a French retailer offers his products on the Internet, it will be equally easy for a Swede as for a French person to access the web page, find out what it has to offer, and eventually order some of the products. Consequently, it is easy to imagine that there may arise cross-border conflicts, that is, legal disputes which involves parties situated in different countries. An action[15] committed on the Internet, whether in form of the collecting of personal data, advertisement of products etc., might be in accordance with the law of one country at the same time as it violates the law of another country. Which country's court shall have the competence to adjudicate, and which country's law shall form the basis for the solution of the material question? These are the issues that are going to be dealt with in the following chapters.

[15] The action in question might be generated both manually or by a computer.

1.2 General delimitations

The subject of this report is to sort out the questions of jurisdiction and choice of law. The object of the report is the TRIP platform, which in simple words is web-travel agent. The framework of the project will not allow a profound analysis, whereas the report will have to concentrate upon identifying some of the more important questions, and try to point out possible solutions to these. Consequently, we will analyse six main fields, i.e. data protection, contractual obligations, consumer protection, intellectual propert right, advertising and liability on the basis of loss suffered due to misleading information. Still, in this report one will have to operate with certain delimitations. It is therefore assumed that:

- It is presumed that the legal disputes are of an international character, see under section 2.
- If the legal disputes are qualified to be a matter of public law, special questions arise in accordance with the application of the rules governing the questions of jurisdiction, choice of law and enforcement. In the following it will therefore be assumed that the legal disputes in question, are a matter of private law. However, this assumption will be suspended to some extent in discussing advertisements on the Internet.
- It is mainly presumed that the legal disputes takes place between parties domiciled within the borders of the EC or the ECCA-states.
- It is presumed that the defendant of the legal dispute is the web shop's responsible institution. Third party conflicts (e.g. liability of intermediaries) fall outside the treatment.

2. AN INTRODUCTION TO PRIVATE INTERNATIONAL LAW

2.1 The problem

When two parties enter into a legal conflict, the usual step is to ask the courts for help. In a normal situation this does not cause any problems. Two neighbours will go to their local court, and this court will use its own rules. However, a problem arises when the two parties do not reside in the same country, or the problem has connections to more than one country.

The problem is defined by a «foreign element»[16], that is not the one of the court. It is in these cases one has to apply the rules of private international law. Private international law basically rules over matters between private parties and not when there is a public element involved.[17]

---

[16] Joachim Benno; *Consumer purchases through telecommunications in Europe*, Complex 4/93 Tano (Oslo 1993), p. 21

[17] In some cases there will be overlap between private and public law. This overlap is normally not an issue in private international law.

In the following we will review some general points of private international law. This is a way of introducing this field of law and the questions surrounding it. First of all, the main questions raised by private international law of jurisdiction and choice of law are discussed. Afterwards we will canvass some of the topics around private international law, like (2.3) the place of private international law in the internal law, (2.4) the name used on the field, (2.5) regulations, (2.6) what to do in case of lack of regulations in this field, by giving an example, (2.7) *renvoi*, (2.8) the limitations of private international law, and finally (2.9-2.11) private international law and cyberspace.

2.2. The main questions

The judges in these cases must, before solving the material case itself, determine two major questions. First of all the court must decide whether it has jurisdiction[18] over the case; i.e. if the parties in question can bring this case into the court. Secondly it must determine what rules to apply to this case. This is a choice of law, and not the application of certain rules to the case. The foreign element in this case gives the court the choice between more than one set of rules. A final question that has importance in interlegal law, is the question of recognition and enforcement. In this report we have chosen not to deal with this problem, mainly because it is often solved under the jurisdiction issue.

To be more practical, if two parties goes to court to solve a legal problem that has a foreign element, the first task of the court is to determine if it has jurisdiction over the parties – which means whether they can render a valid decision with respect to the legal problem. If this is so, the next step will be to decide which law governs the case, i.e. the choice of law. This part consist of several elements. First of all there has to be a classification of the case. It is of great importance if the case is classified as contractual law rather than the law of procedure. When this is done, the court must see if there are some regulations dealing with this problem. If there are not, one has to apply the basic rules of private international law. The result of this will be to determine which country's substantive law governs the question. Once this law has been chosen, the court must primarily use this law to decide on the case. Unfortunately this is not always the end of the process. There may be mandatory rules in the country of the court, which collide with the *lex causae*[19]. In some cases this leads to the use of *ordre public*[20], which requires that other rules be applied. The rules may be either secondary rules of the *lex causae* that are not incompatible with the rules of the court, or rules of *lex fori*[21].

2.3. A part of each country's internal law

It is important to note that even though the name suggests that the rules are international, and valid for several countries, this is not so. Most countries have a private international law, which is a part of their own legal system. And when a case has a foreign element, each court

---

18 Jurisdiction is not always considered to be a part of the private international law, but of the internal procedure law of the country. In these countries, like Sweden, private international law is considered to only consist of the choice of law.

19 The law of the case

20 Public policy of ethical and social character.

21 The law of the court (forum).

should, even ex officio, use these rules. Further down we will come back to the fact that some parts of the world have harmonised some of these rules.

Another important point is that even if the court does apply its own private international law, and then chooses another legal system, there are still some rules of its own that a court will use. Without going any further, this is the court's own rules of procedure and evidence.

2.4. The name of the field

In some countries, the use of the term «private international law» is not common. Instead the term «conflicts of law» is used. This term is usually used by American authors because the conflicts of law in the USA has not been a conflict between national laws, but between the laws of the different states (often called intranational law).

As this report is mainly addresses European conflicts, the term "private international law" will be used in this report.

2.5. Regulations

On the national level, the field of private international law generally has not been regulated in great detail. Certainly there are elements of private international law in several statutes of any countries, or the existing rules are used by analogy. On the other hand, the courts have often filled non-regulated fields. Therefore many of the rules of each country's private international rules are non-written, but they are still valid.

On the international level, there are several efforts to harmonise this field. Examples are the Brussels, Lugano, Hague and Rome Conventions, or the European Convention on Transfrontier Television. Inside the EU, there has been done a great deal of work on harmonising several fields of law. An example is the Directive on data protection. As for the Rome Convention on the law applicable to contractual obligations, this has recently been more or less adopted as formal law by Switzerland. Even so it must be said that these regulations are mostly European. This means that there are great uncertainties when a case involves someone from outside this region.

As for the Lugano and Brussels Conventions, they are similar conventions, solving the jurisdiction in most Western Europe,[22] for cases dealing with private and commercial matters.

[22] The Brussels Convention solves jurisdiction inside the EU, while the Lugano Convention covers the jurisdiction between the EU-countries and some of the EFTA-countries (Norway and Iceland, in addition also Switzerland).

The conventions also solve the problems of these cases concerning recognition and enforcement.[23]

The Rome Convention on the law applicable to contractual obligations does solve the problem of what law governs a contractual obligation between two parties. The principal rule is that the parties have the freedom to choose the applicable law.[24] In absence of such a choice, the rule is to choose the law of the country with which the contract is most closely connected.[25]

The regulations do not always give a private international law solution, but they can also be considered to be a kind of unification of substantive law, especially in the EU. In such situations the conventions or Directives main purpose is to avoid conflict.

2.6. What to do, if in lack of regulations: Methods of solution

If one operates only inside the EU, it is not unlikely that one will find a solution in a regulated law or convention. If not, one will have to apply the general principles of international private law. By this we mean that the court in question does not have any international or European treaties or regulations on which to rely, or any clear national rules to apply. The best explanation is an example.[26] For electronic commerce, the most important field is the one of contractual obligations. This is because the parties in question mainly will try to conclude a transaction on the Internet. One could imagine that there are no regulations in this field, even if the Rome Convention probably will do so. For example:

Assume a Norwegian living in Denmark, contracted in Madrid with a Frenchman (living in Belgium). Assume further that the Norwegian delivered the goods in Germany and has his place of commerce in Sweden. There are many different possibilities as to what law governs this case. Imagine that a court has decided that it has jurisdiction over the parties and that this is a case with a foreign element, one could have these possibilities for the law governing the contract:

- The law of the domicile of the seller (Danish law)

---

23 There are exceptions to the private and commercial matters in art.1(2).

24 Rome Convention art.3.

25 Rome Convention art.4(1).

26 The example is built upon an example taken from the most excellent book by Nikolaus Gjelsvik: *Millomfolkeleg privatrett*. p. 213.

- The domicile of the buyer (Belgium law)
- The law of the country where the contract was finished (Spanish law)
- The law of the country where the contract was fulfilled (German law)
- The law of the place of commerce of the seller (Swedish law)
- *Lex fori* (if the case is brought into a court in another countries)
- The law of the citizenship of the seller (Norwegian law)
- The law of the citizenship of the buyer (French law)
- The law where the contract has it's closest connection.
- The party autonomy, if it is accepted and the parties have chosen a law.[27]

As for this report, the most important of these solutions will later be the one of the closest connection. In contrast to the method of a ''single connection'', which could be solutions like the law of the place where the contract was made, the place of performance or the law according to the domicile or nationality of either the seller or buyer. The closest connection method will be discussed under the section 4.4: Choice of law and liability for economical damage due to misleading information, together with some of the other solutions. In situations where the parties have not made an explicit choice of law in contract, the court might apply the closest connection method. This method implies that all the connecting elements to the contract and the parties are brought together and weighted against each other in order to find the law of the country where the case has its natural seat. For the court, the problem is the weighing of these so-called connections. Because these connections are not stable from case to case, this method is flexible, but unpredictable for the parties.

Looking back at the different solutions, one can see there is a large variety of solutions to a case where there are no direct regulations. In such a case, the court will, if it adheres to private international law, have to look at the different solutions. The next step will be to look at the different arguments. We will here look at different important arguments, but the list is not complete.

---

27 This is the solution of the Rome Convention art. 2.

First, it is important to look at the *predictability* of the law chosen for the parties. A good solution gives every party the possibility to predict the law chosen in the actual case. As an example, the solution of closest connection gives the lowest predictability if there are no directions for what arguments will be used for deciding the closest connection.[28] On the other hand a solution like the closest connection will most likely reduce the forum shopping-effect: The parties will not be able to escape the obvious law of their legal problem.

But there are other arguments that have to be discussed. The possibility for a contributing to *international unity* is important. This means that if this is a solution several countries have adopted, it is probable that other states will use and accept it. And again this reduces the possibility for forum shopping. This leads to another argument, the argument of *acceptance*. It is wise to choose a solution that other countries will accept, especially considering the law of the country of the foreign element. This again leads to the argument of *execution*.

These arguments are not the only one to take into consideration; they are only arguments of principle. In practice the court of jurisdiction will apply *lex fori*[29] to many issues. This so-called "homeward trend",[30] is often used when the court is not too familiar with the private international law. It is also important to note that the court often will consider having sovereignty over the case and therefore applying *lex fori* automatically.

Finally, all arguments taken into consideration, one will have to use one solution. Step two will then be to identify the law applicable to the case; but then again, there are other limits.

2.7. Renvoi

Renvoi is a very special part of private international law. It can come into action if the law chosen is not the one of the court. In such a case it is possible that the law chosen is a law of a country where this county's private international law chooses our *lex fori* as *lex causae*. In such a case, the question is whether to accept this «*renvoi*» or to use the substantive law of this country. If one chooses the first one could end up with a situation where the laws bounce back and forth[31]. In French law this argument is called *argument de la raquette*[32]. On the other hand *renvoi* is not accepted in the Rome Convention art. 15.

---

28 See article by Helge J. Thue in TfR 1965 p.587-610.

29 The law of the court

30 Term often used in the USA

31 This is a not likeable argument against *renvoi* because it does not take into consideration that the case is in one court and it is this court that will accept or refuse the *renvoi*.

32 Gaarder: *Innføring i International privatrett* Universitetsforlaget 1993 (2nd ed.), p.85

Among most European countries *renvoi* is a known question that has nor been abolished, but a choice of law means normally a choice of substantive law. In English law this is the normal idea[33]. The question of *renvoi* will not be any further pursued in this report.

2.8. The limits of private international law – ordre public

Private international law has its limits. First, because all matters of public law are held excluded. Second, there are limits both inside private international law and in other national law fields. The latter can be referred to as the mandatory rules in the law of each country. The boundaries to mandatory rules versus the choice of a law in private international law must be discussed separately in each single case. In cases of consumer protection, the 1980 Rome Convention on the law applicable to contractual obligations has rules on mandatory rules in art. 7, while the *ordre public* rule is stated in art. 16, indicating that these two question must be kept apart. The boundaries to mandatory rules is a part of the choice of law process, while *ordre public* is a process that takes place *after* the choice of law has been made. As for mandatory rules, this report does not pursue this question any further.

What is *ordre public*? Once a *lex causae* is chosen, this is not the end of the matter if the *lex causae* different from *lex fori*. Considering that the law chosen is not *lex fori*, there are possibilities that the court will not accept the application of this law in question because the application of the substantive law will be incompatible with the public policy of the forum. An example of an *ordre public*-rule is the Rome Convention art.16:

> ''The application of a rule of the law of any country specified by this Convention may be refused only if such application is manifestly incompatible with the public policy ('ordre public') of the forum ''

For the rule of *ordre public* to come into action, it is the application of the *lex causae*, i.e. the foreign rule, must be *manifestly incompatible* with the public policy of the forum. For the foreign rule to be *manifestly* incompatible, requires that the application of this rule lead to the exclusion of the rule. If the *lex causae* has provisions that are incompatible with the court public policy, the rule of *ordre public* can not be applied. The qualification of the rule to be incompatible with the public policy is not easy to define. On the other side there are strong suggestions in the European theory that the incompatibility must be between the ethical and social norms of *lex fori* and *lex causae*. In addition these differences between these ethical and social norms must be strong. We do not pursue this matter any further.

Finally it must be noted that if the court applies the rule of *ordre public*, the question is what rules shall then be applied. The choice lies between *lex fori* and secondary rules of the foreign law.[34] Many courts will as a result of *ordre public* collisions apply *lex fori*, mainly to avoid the problem. But how this is done differs. In some cases the court will apply what in

---

[33] Cheshire&North's: *Private International law* (11th ed.) p. 72

[34] It could also be that the applicable law chosen, is secondary rule, and one would then have to look at the primary rule of the law.

Norwegian theory[35] is called *positive ordre public*, meaning that national rules of the court have an ethical or a social norm that can not be in breach of any foreign law, and therefore *lex fori* will apply.

As to this report, we would like to note that in private international law this field is referred to as *ordre public* or public policy in Anglo-American countries. In this report the term *ordre public* will be preferred.

2.9. The application of this field to cyberspace

Unfortunately it is a well-known fact that the courts often disregard private international law. First, the parties often do not have the means to get acquainted with a foreign law by hiring a specialist from a foreign country. Second, the court itself prefers to use its own *lex fori* because this is the law known and because the lack of time does not allow the judge to use more time than necessary on the case. Therefore the question for the future is how the courts in Europe will use the ''instrument of private international law'' on the legal questions that raises from the use of Internet as a commercial marketplace. It is at this point the interesting questions start.

2.10. The international aspect of the Internet

What is considered to be an international case when it comes to cyberspace? When entering cyberspace things change because any contact made over the Internet can be "international". At no point is it sure that if you exchange email with your closest neighbour, this email will go directly to him – it may go across the world before reaching him. This is why the foreign element might be present at all times when using the Internet. Now, if you exchange emails with your neighbour about buying his Rolex, the court will most likely regard this as a national matter. On the other hand, if your neighbour places an advertisement offering his Rolex for sale on the Internet, it is not sure that you will be able to identify him. At this point the matters seems more international, and the court should consider if the case should be solved using private international law. We will not take this argument any further, but it may be a point to argue in front of a court.

2.11. Some points of interest concerning Internet and law

The laws applicable in the analogue world may not be the same as in the digital world. This is important to understand with respect to the question of applicable law. Not only is there is no direct contact between two contracting parties, but also the identification of these parties is not always possible. Many of the laws and acts related to international trade are based on the presumption of direct contact between the parties, and that the object of the trade is physical objects. When using the Internet this is not as obvious. What is contracted, may be sold and

[35] Gaarder *l.c.* p.48

sent over the Internet.[36] This again raises problems of intellectual property rights, which will not be addressed in this report.[37]

In this report we will try to examine the main issues related to private international law and web-shops. This examination will mainly consist of looking at the present regulations, and whether they are applicable to the issues in question. For some issues there may be some regulations developed especially for a digital environment, which then will be applicable. On the other hand there might be issues where it will not be possible to apply current regulations. Here the question will be what alternative solutions can be found. The first solution is to consider if the traditional regulations can be adapted. This will in general mean to try to identify the parties in question and their places of attachment. If this is not possible, we will have to rely on the traditional private international law, and to explore the consequences of their possible application. However, at this point we will be arguing mainly on the basis of legal policies.

3. JURISDICTION

3.1 Introduction

When a legal dispute enters the court, the court will have to decide whether it has the competence to adjudicate in this specific case. Concerning courts within the area of the EC and the ECCA-area there are two conventions, which in many cases will provide a solution to the questions; the Brussels- and the Lugano Conventions. All the member states of the EC have become parties to the Brussels Convention of 27 September1968. Furthermore, all the ECCA-states (with the exception of Liechtenstein) have become parties to the Lugano Convention of 16 September1988, which for our purposes may be seen as identical to the Brussels Convention with respect the material content. The two conventions will be treated as one in the following.[38]

The conventions only provide solutions for cross-border disputes concerning "civil and commercial matters",[39] that means legal disputes as part of *private law*. In the ruling of the

---

[36] There are great advantages doing so. Notably the expenses and the wrapping, i.e. buying music over the Internet in the future will not consist presume the purchase of a physical object like a CD, but the transfer of a file over the Internet.

[37] Jon Bing: *The identification of applicable law and liability with the regard to the use of protected material in the digital context* (E-CLIP draft report).

[38] Reference to articles in the following, will be based upon the provisions laid down in the Brussels Convention.

[39] Art. 1 (1)

EC-court *LTU v Eurocontrol,*[40] it is stated that essential for the qualification is the character of "the legal relationships between the parties to the action of the subject matter of the action". In other words, it is only in situations where a public authority has exercised public authority, that the provisions is inapplicable. The qualification of whether a legal relationship is to be deemed a matter of public or private law, is to be determined on the basis of an autonomous interpretation of the Convention, where respect shall be paid to the purpose and the structure of the Convention, and also the shared principles that can be extracted from the legal systems of the parties to the Convention.

As concerning the enforcement of advertisement legislation, this typically will be considered a matter of public law, and thereby fall outside the scope of the conventions. The treatment of the jurisdiction as it comes to the questions concerning the enforcement of advertisement legislation, therefore will be dealt with in a separate point, see sect. 3.3.

3.2 Jurisdiction in matters of private law

3.2.1 The point of departure

As a point of departure, the defendant is to be sued in the courts of that state where his business has his seat. In order to determine the seat, the court shall apply its own rules of private international law.[41] In our context, the provision does not generate any special problems, and consequently further analysis can be avoided.

3.2.2 Special provisions

In certain cases, alternative provisions may determine the jurisdiction. The most interesting in our context are:

a. Matters relating to a contract, art. 5 (1)

b. Matters relating to consumer contracts, art. 13

c. Matters relating to tort, art. 5 (3)

The provisions are alternatives to the provisions in art. 2, which implies that the plaintiff can decide whether to sue in the country of the defendant or in courts of the country that follows from the rules laid down in the special provisions.[42]

---

[40] Decision of October 14th, 1976 in Case 29/76, LTU v Eurocontrol [1976] ECR 1976; Concerning the Brussels Convention.

[41] Art 53 (1)

[42] Provided that this will be a different jurisdiction

Matters relating to a contract

According to art. 17 the parties may determine a court to have exclusive jurisdiction, simply by agreeing upon it. Such an agreement must be either a) "in writing or evidenced in writing", or b) in a form "which accords with practices which the parties have established between themselves", or c) in a form "which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned".

If the parties have not chosen a venue in accordance with art.17, provisions are given in art.5, which seeks to point out the right jurisdiction. Art. 5 (1) states that a person can be sued "in the courts for the performance of the obligation in question". The EC-court has decided that the relevant obligation does not necessarily have to be the characteristically performance of the contract (typically: the merchandise to be delivered). A contractual relationship will nearly in all cases consist of several obligations of different character. This may lead to the fact that there might be operated with several *fora solutionis* to the same contract, that is places where the respective obligations are to be performed.

In determining what are to be considered as relevant obligations, the decision of the EC-court in *De Bloos v Bouyer*[43] must be considered. The decision makes a distinction between primary and secondary obligations of the contract. The secondary obligations are defined as having the character of sanctions, which replace ordinary obligations of the contract (the qualification is done on the basis of national law). It is only the primary obligations that are relevant for determining the jurisdiction. The decision has been criticised, but nevertheless must be seen as an expression of contemporary law, as the decision has been followed up by the court in later cases, also the wording of the provision supports the result of the decision.

It might be that the defendant, in the contract between the parties, has obliged himself to handle the collected or extracted personal data in a specific manner. Given that these obligations are defaulted, it may be argued that the obligation in question is the basis of the dispute, and that the place where this obligation is to be performed can be chosen as an alternative venue. Similar considerations can be made if the defendant in the contract has guaranteed the accuracy of the information provided, and the customer suffers an economic loss because the information proves to be incorrect. It is likely that a court will hold that obligations like those mentioned above must be qualified as a primary obligation. Consequently, the courts of the country where the obligation in question is to be performed will be competent to adjudicate.

The problem therefore consists of determining at what place obligations like those mentioned above are to be performed. The solution will specifically depend on whether the place of the performance are agreed upon by the parties or not.

If the parties have agreed upon the place of performance of the obligations in question, the parties are bound by the agreement.[44]

Given that a valid agreement between the parties does not exist, the Convention does not provide any solutions to the problem in our context. There are likely to exist national differences when it comes to determining what place is to be considered the place of performance,

---

43 *De Bloos v Bouyer* , 1976 ECR 1497

44 *Zelger v Salinitri I,* 1980 ECR.

and accordingly it will be impossible to give a definitive answer to what is likely to be the result in an actual case. One will therefore have to calculate with the risk that obligations like the one mentioned, can be argued to have universal relevance. That would mean that their compliance not only would have to take place in the countries of the seller and buyer, but potentially also in all other countries in the world. If such obligations are violated on the Internet, one will easily submit one self to the situation where the courts of practically every nation in the world will have the potential to adjudicate.

Matters relating to consumer contracts

When it comes to contracts where one party is professional and the other a consumer, special rules are given in section 4(2), which places the consumer in a more fortunate position. We will only examine the provisions which has the greatest importance in our context.

If the conditions set out in art.13, first paragraph, third point, letter a and b are fulfilled, the consumer may bring proceedings against the service provider either in the courts of the state in which that party is domiciled, or in the courts of the state in which he himself is domiciled. Further, proceedings may only be brought against the consumer in the courts of his home country. The mentioned conditions in art.13 are as follows: Firstly, the consumer, before concluding the contract, must have been subject to a special invitation, or advertising, in the State of his habitual residence. Secondly, he must have taken all necessary steps on his part for the conclusion of the contract in that country. These are the same conditions that are set out in the Rome Convention, concerning the choice of law questions. To avoid treating provisions with the same material content twice, we therefore refer the reader to the chapter concerning choice of law and consumer protection, see **4.?

The provisions are mandatory and generally may not be departed from by agreement[45].

Matters relating to tort

As for matters relating to tort, the courts of the country for the place where "the harmful event occurred", will have jurisdiction, art. 5 (3). The EU-court has stated that one has to establish an autonomous understanding in the interpretation of the expression "the harmful event occurred".[46] Furthermore the EC-court has interpreted the expression to also include the place where the effects of the harmful event took place, see *Bier v Mines de Potasse d'Alsace.*[47] In the case *Sheville v Presse Alliance*[48] there is given a general definition on what might be seen as the place where the effects of the harmful event took place. This is the place where the harmful event has caused damage to the injured party. These guidelines must be

[45] Art.15

[46] *Marinari v Lloyds Bank,* 1995 ECR 1-49.

[47] *Bier v Mines de Potasse d'Alsace,* 1976 ECR 1735

[48] *Sheville v Presse Alliance, 1995 ECR*

presumed to have relevance also when it comes to actions committed on the Internet. In the determination of the venue, one shall not include consequential damages or loss in the consideration. This is stated in the decision *Dumez Batiment v Hessische Landesbank.*[49]

It must therefore be presumed that contemporary law holds that in every country where the injured party has suffered loss due to the harmful event, the courts will probably have competence to adjudicate.[50] This is also goes for the situations where the responsible action was committed in the context of the Internet. In the doctrine it is presumed that also loss of a non-economic nature, like compensation for damage of a non-economic nature or compensation for defamatory statements etc., sets out the right to adjudicate in accordance to art. 5 (3)[51].

Concerning violations of intellectual property rights committed on the Internet, it has been stated by some authors that the competent countries must be limited to only incorporate those countries to which, on the basis of an objective assessment, it seems likely that the copyrighted material will be downloaded.[52] According to this consideration it will only be the courts which have their judicial district within the "targeted area" that have jurisdiction. It might be questioned whether a similar limitation must be applied also for other types of infringements. The question will not be pursued here since it is doubtful whether the above listed presumption can be seen as an expression of current law. However, there might be reasons to note that if the presumption is to be followed by the courts, it is likely that similar considerations would apply also to other kinds of infringements. The condition for applying the same considerations is of course that it is possible to stake out a specific "target area".

3.3 Jurisdiction in matters of public law - legal disputes concerning claimed violations of advertisement regulation

With respect to the application of the regulation of advertisements, it is mentioned above that this typically will be considered as being part of public law. The reason is that the advertisement regulations are enforced by public administration. The legal dispute therefore lies outside the scope of the conventions. The question that emerges is which rules will then apply in determining the jurisdiction.

It is an acknowledged principle that when dealing with public law a state can only assume jurisdiction if the assumed infringing event falls within the scope of national legislation. One will therefore have to interpret the application of every single national regulation. Such an analysis exceeds the basis of this report, and consequently will not be undertaken.

However, there are reasons to believe that an essential criterion will be whether the advertisement has taken place within the *territory* of the country. For these reasons, the question will be how such a criterion is to be applied for advertisement on the Internet.

At the first glance this may seem trivial. Advertisements on web pages are capable of being viewed in all European countries, and one might therefore say that the medium, which is cho-

---

[49] *Dumez Batiment v Hessische Landesbank,* 1990 ECR 1-49.

[50] However, an important limitation lies in the fact that it is only possible to seek compensation for damages which didn't occur within the territory of the country.

[51] *Stein Rognlien Luganokonvensjonen – norsk kommentarutgave* p. 147

[52] Andreas Fuglesang and Georg Krogh *"Internett og jurisdiksjon"*, 1998 (ms)

sen to display the advertisements, should not determine the application of legal rules. However, the way that the advertisement is transmitted on the Internet may create problems. This is because the retailer himself does not commit any *active* actions in order to distribute the advertisement to a certain country. It is the end-user who makes the connection to a database containing the web page in question, and thereby initiates the transmission, so that he finally will have the advertisement displayed at his own screen. Is it then, under these circumstances, plausible to state that the advertising is taking place within the territory of the country where the end-user is located?

Imagine that a Swedish court claims that their national legislation governing advertisement is violated by an English retailer who has his database on a server geographically located in United Kingdom. It might then be argued that the advertisement is taking place on the server located in United Kingdom, and therefore will not fall within the scope of the Swedish regulations.[53] The fact that a Swede through establishing a connecting to the database has the commercial displayed on his own screen, cannot be the retailer's problem as long as the retailer in question has not made any active attempts to transmit the commercial to Sweden. One might say that the situation will have to be placed on equal footings with situations where a Swede during a vacation in London buys a magazine containing advertisements which are forbidden by Swedish legislation and brings the magazine back to Sweden.

However, it is not certain whether a court will accept such a formal consideration. It may be maintained that when a retailer chooses to advertise his products on the Internet, he must be aware of the potential of the advertisement being displayed on all screens connected to the Internet, and that the reality therefore is a worldwide promotion of his product. This was probably also the idea of choosing exactly this specific medium. It may therefore seem inconsistent that retailers who utilise the Internet as a medium to promote their products shall be put in a more favourable position than the ones that utilise more traditional media for the promotion.

It is uncertain how the question will be solved. It is likely that the way the national courts solve the problem will depend greatly on to what extent they feel obliged to lay down a strict understanding of the wording of the provisions.

4. CHOICE OF LAW

4.1. Data protection and choice of law

4.1.1. Introduction

Data protection will be in the future, as now, an important issue in a digital society. Increasingly personal data is being stored on computers that are connected to other computers. The possibility for people to access this information across jurisdictional borders is also in-

[53] *Joachim Benno* "Consumer Purchases through Telecommunications in Europe", Complex 4/93 Tano (Oslo 1993).

creasing. This, in turn, increases in the potential for choice-of-law issues arising with respect to regulation of the information processing concerned.

The following analysis rests on several presumptions. First, we presume there is an issue involved which has a certain international, or foreign, element, thus allowing the issue to be considered a question of private international law. An example is a Web-shop, which collects data about customers who are not situated in the same country as the owner of the Web-shop. The TRIP platform, as an Internet travel agent, will as we have supposed it, be such a Web-shop, offering tickets to customers around the world.

Second, we presume that the matter is of a private character. By this we mean that the parties presenting themselves to the court do not include government agencies.

Third, we presume that the matter occurs within the geographical area of the EU/EFTA countries that have signed the Lugano and Brussels Conventions.

Fourth, we presume that the parties have been identified, and that the transactions between the parties did not occur anonymously.

Finally, we presume that the aim of this analysis is to allow the owner of the Web-shop to be able to predict more precisely which law will regulate the processing of data about his customers.

4.1.2. The regulation of this field inside certain areas

Every EU/EFTA state has enacted data protection legislation. Furthermore, the EU has adopted a Directive on data protection (Directive 95/46/EC – hereinafter abbreviated "EC-DPD") which is aimed at harmonising data protection regimes inside the EU. This Directive will also be highly influential for the development of data protection law in EEA states that are not members of the EU – i.e., Norway and Iceland – especially once the Directive is formally incorporated in the EEA Agreement.

4.1.3. The Directive's impact on Internet-shopping

The EU DPD applies to "the processing of personal data wholly or partly automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system" (art. 3(1)). There are certain delimitations to the applicability of the Directive laid down in art. 3(2) but these are not relevant to the analysis here.

The Directive will apply to all types of web-shops, like the one of TRIP, when this collect and further process data that is "personal" pursuant to art. 2(a) of the Directive. Art. 2(a) defines what is "personal data" as follows:

> 'personal data' shall mean any information relating to an identified or identifiable natural person ("data subject"); directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; ....'

In light of this definition, it is quite possible that the information by the TRIP platform about the customer could be considered as "personal". In most cases airline customer must give a huge amount of information about themselves to the airline. For further discussion of this issue, see the IMPRIMATUR-study by Lee Bygrave and Kamiel Koelman.[54]

4.1.4. The law applicable to the processing of data

The next point is to identify the law applicable to the handling of the database and the data concerned. According to art. 4(1)(a) of the Directive:

> 'Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where ... the processing is carried out in the context of the activities of an establishment of a controller on the territory of the Member State ...'

As to who is the controller, this is defined by art. 2(d) as:

> 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data ...'

This means that the responsibility for observing the rules laid down in data protection law is given to those actors that control the means and purposes of the processing of data on other persons. Note that art. 2(d) envisages that there can be more than one controller per data-processing operation. Further, it is factual control over, not possession of, the data, which is the main criterion for being a controller.

Of decisive importance for working out which law is to be applied to a given data-processing operation, is the meaning of the term "establishment" in art. 4(1)(a) of the Directive. Some light is cast on the meaning of the term in recital 19, which states:

> 'Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or subsidiary with a legal personality, is not the deter-

[54] L A Bygrave & K Koeman: *Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems* (Amsterdam: Institute for Information Law, 1998), p. 13. The report is also available via URL <http://www.imprimatur.alcs.co.uk>.

mining factor in this respect; whereas, when a single controller is established on territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities; ...'

At this point, the principal rule must be said to be clear in the case where we have one controller with only one place of establishment: the applicable law will be the law of that place of establishment. This means that if a controller has headquarters in country A, the data protection law of country A will apply.

Problems arise when the controller is established in several jurisdictions. We will address these problems below.

4.1.5. Problems of the Directive

In this section, we will look at the problems resulting from a situation in which the controller is established in multiple jurisdictions. Second, we will consider the issue as to whether data mining can be considered as involving a contract between the controller and its counterpart. Finally we will look into the problem of *ordre public*[55].

Problem 1: The controller has more than one place of establishment

As we have seen in sect. 4.1.4, it is quite clear that an "establishment" may include subsidiaries, branch offices, and perhaps also agents or similar representation. This means that if the controller has a main office in one country, and several branches in some other countries, different laws will be applicable to a single data-processing operation that extends across borders.

To be more specific, we can imagine one controller, A, situated in country A, exchanging information with its sub-branch, B, in country B. The collection (or mining) of this information can take place from almost any country. If there is no exchange of information, the data processing in country A will first have to comply with the data protection law of country A, and the data processing in country B will have to comply with the data protection law of country B. If B sends information to A, the situation changes. From the wording of art. 4(1)(a), the data protection law of country B will still be applicable to the case, even if the information now is in the hands of A. This rather complex situation could mean that A would have to separate all information according to where they come from, or comply with the strictest data protection law at the time. Inside a large community,[56] this means that one would at all times have to be looking at the possibility of new regulations and change internal routines.

But this problem has also another aspect: that is, a positive conflict of jurisdiction might arise. According to Bing:

"The national data protection law of country B may, due to the close co-operation with the processing taking place at the main office, give its law extraterritorial application to the op-

55 Cf. Sect 2.8

56 Now counting 18 countries, and we do not include the two non-EU EEA-countries.

eration in country A. The result will have to be that the controller has to comply with the legislation of both country A and country B. As the law of both countries are harmonised by the Directive, this probably will not be too difficult, but due to the leeway of national choice in the implementation, one may have provisions which are in conflict in such a way that they cannot simultaneously be fulfilled – in this case the controller is in trouble."

We do not pursue this question any further, but the controller must be aware of the difficulties concerning implementation of the Directive.

Until now we have taken for granted that there is only one controller and that this controller has one or several sub-branches situated in different countries. But, as noted above, art. 2(d) of the Directive seems to presume that there may be more than one controller per data-processing operation. In cases where this occurs, we may again be faced with a situation in which one set of data or one data-processing operation is subject to different national laws. This will not be a problem if the laws are in harmony – which is the assumption of the Directive – but such harmony might not eventuate given that states are given a significant "margin of appreciation" in implementing the Directive.

Problem 2: Can data mining be considered a contract between the data subject[57] and the controller? Can the contract derogate from the provisions of the Directive?

To the first question, it is quite clear that even a small web-wrap clause will be difficult to view as a contract. However, if the controller collects this information by, for example, a customer filling out a purchase, order or subscription form on the Internet, and the controller sends the customer a password to permit entry to the rest of the web-site, it is at least arguable that a contract has been made that is binding for the customer. It would be too speculative to attempt to draw any firm conclusions on this point, but it is probable that Continental-European conceptualisations of what constitutes a contract will be more restrictive than Anglo-American conceptualisations.

As for the second question, the Directive makes clear that one of its basic purposes is to protect human rights, in particular the right to privacy. This follows from art. 1(1):

'In accordance with this Directive, Member States, shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data …'

It also follows from recitals 3, 7, 8 and 9 in the Directive's preamble. Accordingly, it could be argued that the Directive intends to set a "bottom-line" for protection of individual persons' fundamental rights. Thus, any contract which attempts to derogate from this bottom-line will probably not be tolerated, unless the controller "adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals …" (Art. 26(2)).

Problem 3: Can the rules of ordre public stop data mining?

It is possible to envisage a situation where the court has given the parties jurisdiction and made a choice of law that is not the law of the jurisdiction in which the court is established; i.e., *lex fori*. If the law chosen offers a level of data protection far below that offered by the jurisdiction in which the court is established, there is a possibility that the court will refrain

---

57 The data subject is the person to whom data relate; cf. art. 2(a) of the Directive.

from applying the chosen law by reference to *ordre public* considerations. This possibility will increase the more the personal data concerned are sensitive and in need of stringent protection.

4.1.6. TRIP and data protection problems in a private international law context

If one should come to a conclusion, concerning TRIP and data protection, one could in short comment on the fact that, as we have understood TRIP, will imply the use of personal data. These personal data is given to TRIP, as an "INTERNET – TRAVEL AGENT", whereas TRIP will have to transmit the information to the airline company.

The first problem concerning private international law, is the handling of personal data comming from abroad. As TRIP is Internet based it is possible to reach it from any parts of the world, but as a result in Europe, the handling of personal data will must comply with the data protection of the country where TRIP is located(meaning the branch of TRIP the customer has contacted). This might cause some problems, because there are after all differences in the different data protection acts. They are maybe minimal, but they still exist. Outside Europe, the situation is more unshure. If the TRIP platform does not comply with the Malaysian data protection act, and a Malaysian customers purchases tickets from TRIP, the outcome of such a case, having jurisdiction in Malaysia, is not unlikely to have Malaysian law as applicable law.

The second problem, and in fact much more serious, is the handling of data, when TRIP passes on the information to the airline.

4.2. Choice of law in contracts

4.2.1. Introduction

As already described in this report the TRIP platform is reservation system for travel reservation and interactive purchase. This means that there are customers approaching the TRIP platform, and they are interested in buying travel tickets. Between the customer and TRIP the conclusion of a purchase will be a contract normally saying that the customer has committed himself/herself to buy X tickets to the price of Y, and that TRIP has committed themselves to deliver this/these tickets.

The great advantage of the TRIP platform is the global presence of this platform through the Internet. This would again imply an international diversity of actors in the contracts. As to the contract, the main question from a private international law point-of-view, is what law applies to the contract when this is an international relation between the customer and TRIP. In this part of the report, we will try to raise questions around this theme, and if possible answer them.

Initially we would like to point out that this part of the report is only concerned with the traditional aspect of a contract. The TRIP platform can both have a business-to-business as-

pect and a consumer-to-business aspect. As to the consumer protection problem, this is left out in this part of the report, and is in it self a main aspect of this report. In this part we will focus on general aspect of what law is applicable to the contract of the buyer-seller. The report is only concerned with TRIP contracts within the European borders, which also means that the main objective of this part of the report will be the 1980 Rome Convention on the law applicable to contractual obligations.

In this part of the report we will firstly concentrate on the international aspect of the TRIP platform. Secondly, and which is also the main issue here, we will focus on the choice of law within the parameters of the 1980 Rome Convention. Thirdly, we will focus on the validity of the contract. Finally, we will only briefly discuss the aspect concerning mandatory rules and ordre public, without discussing consumer protection problems.

4.2.2. The international aspect of a TRIP-contract

In the introduction of this report we only briefly mentioned that one of the problems of private international law was how to qualify a case of being a part of private international law. The key point was the presence of a "foreign element". In a traditional contract within the TRIP platform, it is natural that the contract has this foreign element. For example; a Frenchman purchasing a ticket from the SABENA airline on the TRIP system, situated in England. Consequently, this will be a matter for private international law to solve what the choice of law will be.

Nevertheless, there are other points to this question that raises a far more serious problem. The problem we are referring to is the problem of the Internet. This is because the Internet in it self is a foreign element. The question is whether the foreign element of the Internet automatically is enough to qualify the case to firstly be solved by private international law.

Accordingly, if a situation arises where an Englishman purchases a ticket from British Airways on the TRIP platform, the purchase is still Internet based, and therefore the global attachment is present. Technically, there are possibilities for the Internet message from the buyer to be sent around the world before reaching the seller. Practically, entering the Internet one can not always be sure if the counterpart is from any particular country. Addresses on the WWW with endings like www.nnn.com, can be from a number of countries, but the origin of the website-owner is not understandable. Consequently, this should lead to the conclusion that any transaction made over the Internet has a foreign element that implies the application of private international law.

However, inside the European Union the 1980 Rome Convention on the law applicable to contractual obligations, Art. 1 states:

> "...rules of this Convention shall apply to contractual obligations in any situation involving a choice between the laws of different countries[my underlining]..."

In the Report on the Convention on the on the law applicable to contractual obligations by Mario Giuliano and Paul Lagarde, Art.1 explains the foreign element as:

"...It must be stressed that the uniform rules apply to the abovementioned obligations only "in situations involving a choice between the laws of different countries". The purpose of this provision is to define the true aims of the uniform rules. We know that the law applicable to contracts and to the uniform rules. We know that the law applicable to contracts and to the obligations arising from them is not always that of the country where the problems of interpretation or enforcement are in issue. There are situations in which this law is not regarded by the legislature or by the case law as the best suited to govern the contract and the obligations resulting from it. These are situations that involve one or more foreign elements to the internal social system of a country. E.g, the fact that one or all of the parties to the contract are foreign nationals or persons habitually resident abroad, the fact that the contract was made abroad, the fact that one or more of the obligations of the parties are to be performed in a foreign country, etc. And thereby, giving the legal systems of several countries claims to apply. These are precisely the situations in which the uniform rules are intended to apply..."

This would imply that a situation where the parties of a contract are only connected to one country, then they should not have to apply private international law. On the other hand, the 1980 Rome Convention was not intended for a international situation like electronic commerce over the Internet.

Nevertheless, the goal of this discussion is to raise the potential questions. The international aspect of the Internet should not be underestimated. Some courts will at all times try to apply national rules, and in such situations the weight of the Internet will be low. On the other hand, the raise of the electronic commerce will in turn lead to an increased number of Internet related courtcases. It is our opinion that the use of private international law will then increase largely.

4.2.3. The choice of law in contracts

4.2.3.1.General

The choice of law in contracts in the context of private international law, has a long history. The development of this field of law in the world has been more or less the same during the 19th century. Both in theory and in the courts, one sought a single connection as to the choice of law. These single connections could be like the place where the contract was signed[58], implying *lex loci contractus*. Others are the law of the place where the contract was fulfilled, *lex loci solutionis*, or the law of the debtor's domicile. In the 20th century the party autonomy and the method of the closest connection have been accepted as the principal rules.

[58] For Internet related cases, this would be difficult, because the signing is difficult to relate to one specific place. This could be the place where the

The scope of this report is the European Union, including the European Economic Area-countries. Inside this spectrum, the most relevant document is the 1980 Rome Convention. The report on the Convention can also be of great help in understanding the Convention. Unfortunately there is very little courtcase material on the Convention.

The main question concerning the Rome Convention is its applicability towards Internet related contracts. The use of such an instrument as the Internet for contracting was unthinkable when the Convention was signed. On the other hand, the Convention is the result of traditional private international law, and thereby the most natural reference as to how to solve such questions. Consequently, we will look into the problemacy of this Convention and its application to Internet contracts.

4.2.3.2. The principal rule of the Rome Convention: Party Autonomy

a. The Rome Convention

The principal rule of the Rome Convention is stated in Article 3(1) of the Convention:

> "...A contract shall be governed by the law chosen by the parties. The choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or a part only of the contract..."

b. The reasons behind the party autonomy

The principal rule of the Convention is the freedom of choice of the parties. Meaning that they can chose the law applicable to the contract. This so-called party autonomy[59], has its roots, in an international perspective, back to the 1955 Hague Convention. In Europe the party autonomy has been fully accepted for many years, and in Italy as early as 1865 when it was enacted. The parties freedom to choose the law applicable is also supported both by arbitration decisions and by international treaties designed to unify certain rules of conflict in relation to contracts. The party autonomy implies that the parties can make a choice of law, like for example with a choice of law clause in the contract. This choice of law must not be mistaken for a choice of jurisdiction clause, which makes a choice as to the court which shall govern the case. According to the Report on the Rome Convention, a choice of jurisdiction clause is not legal because it is considered being a part of a country's public law. The choice of law is also solved by the Brussels and Lugano Conventions, as formerly explained in this report.

One might ask why should the court accept the party autonomy? There are several reasons to this in the law history. First of all, the courts have as already mentioned historically ac-

[59] In French called *autonomie de la volonte.*

cepted the party autonomy. They have tried to find the hypothetical choice of law[60] of the parties. Secondly, the party autonomy have been stated in several cases all around the world[61], evolving from just being the possibility for a incorporation of foreign provisions to the acceptance of a full party autonomy as to the choice of law in the 1955 Hague Convention. Even though the party autonomy has its problems against mandatory rules, there are some strong reasons for accepting it for more than historical reasons. These other reasons are, first of all, predictability. There is a strong need for the parties to have a knowledge about the outcome of their case. Secondly, as the parties are closest to the case, their knowledge of their own situation, implies that they know what law is most suited for their case. Both these reasons are heavy arguments as to accepting the party autonomy.

c. The form of choice

As to the choice of law, it is stated that is must take place under a certain form. This is according to the Convention: "...expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case...". This should indicate that there are to choices as to how the part autonomy can take place. First of all, the parties can directly make a clear choice of law clause in the contract. Secondly, "the circumstances of the case" might give the choice of law. As to the former, this could be the easiest task. The parties could make a clear statement in the contract saying: "We, the parties of this contract, hereby chose xxx law to be applicable to this contract". In a business to business relationship, such a clause will be natural and in most cases acceptable for the court. Accordingly, the TRIP platform will be ideal for such a clause for the business buyers. However, if the buyer is a private person, meaning a consumer. The choice of law clause might be invalid as to the consumer rights. This question will be further persuaded in the section about consumer protection. As to the latter problem, about "the circumstances of the case", this causes generally more problems. The article indicates that if there is no clear choice of law clause, there might still be a indirect choice of law made in the contract. The choice of law must be "...demonstrated with reasonable certainty..." according to the report on the Convention. The reasonable certainty of this choice of law, is restricted to contracts where the parties indirectly have made such a choice, but not expressed in a clause. The report on the Convention gives certain examples: "...the contract may be in a standard form which is known to be governed by a particular system of law...such as a Lloyd's policy of marine insurance...in other cases a previous course of dealing between the parties under contracts containing an express choice of law may leave the court in no doubt that the contract in question is to be governed by the law previously chosen where the choice of law clause has been omitted...". It is also probable that if the parties have

---

[60] See Erik Siesby: *Lærebog i International privatret – Almindelig del og formueret(2.udgave), København 1989, p. 77.*

[61] Here some few examples: American case: *Gerli&Co. Vs. Cunard S.S.Co (1931) 48 F 2 d 115 (2 Cir.).* English case: *Dobell&Co. V. Steamship Rossmore Co. 1895 2 Q.B 408, 413 (C.App) and Vita Food Products Inc. V. Unus Shipping Co.(1939) A.C. 277 (P.C.).* The latter case is a very famous case that has been strongly criticised, where Lord Wrights dictum stated: "...It is now well settled that by English law,...the proper law of the contract is the law is the law the parties intended to apply...". Unfortunately, the Lord did set a limit to this party autonomy: "...provided the intention expressed is *bona fide and legal*, and provided there is no reason for avoiding the choice on the ground of public policy."

chosen a jurisdiction, this can lead to the idea that there has also been a choice of law. All these examples, only to show that the choice of law has to have a certain precision. However, it would be unwise to try to indicate a precise limit for what can be said to be a demonstration of a choice of law. Nevertheless, a clear case where there is not a direct or indirect choice of law, is when the court tries to find a hypothetical choice of law. This is not a choice of law, and is more related to the Conventions Art. 4 on the closest connection.

d. The question of severability (depecage)

The main idea behind choice of law is that one law governs the hole contract. The contract can not be divided into small pieces, with each, its own law. The 1980 Rome Convention, has as principal rule that one law governs the whole contract[62]. However, there are exceptions to this *unity*, mainly, in the last part of Article 3(1) of the Convention. The reason behind this is the part autonomy, meaning, the parties must be able to chose the law they need, to those parts of the contract that have such needs. If that means switching laws, this must be accepted. The makers of the Convention had in mind the large contracts, involving several sub-contacts.

Now, what kind of choice of law can there be? In this part we exclude the discussion concerning mandatory rules. The latter, will be discussed later on. The primary issue is the last part of the Convention Art. 3(1) stating that the parties can select the applicable law "...to whole or a part of the contract..." Firstly, it is most likely that this will only relate to the part where the parties have made a clear choice of law. This is because, if there is no direct and express choice of law clause, it will be very difficult to identify to which part of the contract the different laws will apply to. Secondly, the Convention clearly states the freedom to make a choice of law clause with different applicable laws at the end to different parts of the contract. In some cases this is a great advantage, e.g. in contracts involving different sub-contracts. In contracts involving shipment overseas, it is quite thinkable to both have a choice of law clause to the general contract and a choice of law clause as to the shipment itself. However, for a type of platform that TRIP presents, there are several dangers in forming this type of choice of law. There are limits to what could be considered being an attempt to escape the proper law of the contract, also known in French as *fraude à la loi*. This notwithstanding, that because of the party autonomy *fraude à la loi* is more unlikely when it comes to contractual obligations[63]. Furthermore, this type of choice of law clause can also cause problems concerning consumer protection. Different applicable laws, is a strong indication for these sorts of problems, and especially for consumer transactions, TRIP should avoid such clauses.

e. The time when the choice is made

The next question is when can this choice of law take place? According to the Art. 3(2) of the Convention, the parties have full freedom as to when the choice of law can be made. As a result, the choice of law can be made after the conclusion of the contract. However, there are

[62] See, Erik Siesby, p. 67.

[63] Henri Batiffol/Paul Lagarde: *Droit international privé I,* Paris 1981, p 429.

limits to how long this choice can be made. After the start of the case in the forum, it is the procedural law of this forum that decides how until what point the parties can chose the applicable law. This goes to prove the importance also to the question of jurisdiction, previously mentioned. Finally, as to the TRIP platform, it can be said that if the platform does not include a choice of law possibility for the contracting parties, there are possibilities to make this choice later, but then the parties again have to come to an agreement. If they do not, the answer will be the method of the closest connection in the Art. 4 of the Convention.

4.2.3.3. The closest connection method – when no choice have been made

In those cases where the court can not identify if the parties have made a choice of law, the parties could seem to be in lack of an applicable law. In some countries the court will automatically apply lex fori, as a form of "homeward trend". However, this is most unsatisfactory, as it would implement a forum shopping situation. The 1980 Rome Convention therefore states in Art. 4(1):

> "...To the extent that the law applicable to the contract has not been chosen in accordance with Article 3, the contract shall be governed by the law of the country with which it is most closely connected..."

a. About the method

The main problem is to identify the law that is most *closely connected*[64] to the case and the parties. The great advantage of this method is its flexibility. As to the method, one therefore has to identify the persons behind the case, and their means of communication. In the case of TRIP, on one hand one has the customer, private or business, situated in one country. The operator of TRIP situated in one country, and maybe the technical means are situated somewhere else. The airline is also situated at a certain point, or at least its headquarters. The departure of the flight can also be different from the place of domicile of the customer, nor without mentioning the destination. All these elements mentioned will give a certain connection to the case. There are of course other points, like the language of the contract, and the negotiation, but the main issue here is to show that all these points are relevant to the closest connection. How the court will weigh these different points against each other belongs, however, to the uncertainty and unpredictability[65] of this method. In some cases the court will try

[64] The method of the closest connection has several names. In Denmark it is refered to as *"den individualiserende metode [the individualizing method]"*, while English law and American law, respectively refers to this as *"the proper law of the contract" and "the centre and gravity method"*.

[65] The method of closest connection is severely criticised by Prof. H.J.Thue in *TfR 1965 p.587.* In Norwegian Private international law, this method is refered to as the IRMA-MIGNON-formula, concerning two Norwegian ships colliding in the Mouth of Tyne, and where there was a difference between the maritime law of England and Norway with respect to the liability. Here there was no doubt that the 'injury' took place in British territory,

to look for a solution that pleases them, namely weigh the arguments so that they can apply lex fori. This is often refered to as the "homeward trend". This report, however, does not give us the possibility to make a lager debate on how these different connecting points might react one against the others.

The method of closest connection has its disadvantages, and should therefore be avoided. Here, we would just like to point out that the method suffers from a huge unpredictability. First of all, concerning the how the different connections will we weighed in each court. Secondly, and maybe even more important, concerning at what time this closest connection decision shall take place. As a consequence for electronic commerce like TRIP, one can imagine different solutions concerning the time one wants to decide the closest connection. Without going any further, the decision point could be any time from the point where the customer decides to reply to an Internet offer, TRIP confirms the tickets at their place, the ticket is issued from the company, the departure of the flight, the destination point, or finally the billing (if the billing takes place after the flight). This is an important uncertainty of the case.

By contrast, as to the different connecting points, one can make a distinction between subjective and objective connections[66]. The former relates to connections like the wishes of the parties, their understanding of the contract, the language of the contract, references to legal systems or acts. The latter refers to connections like the place of agreement, place of fulfilment of the contract, the different parties domicile or place of trade. In electronic commerce, these places can rely to different solutions. Hence, the technical connections will play a major role of the decision where the closest connection is made. Questions like, where the contract was signed/agreed or where the contract was fulfilled have a relevance to where the server is situated, and where the place of commerce of the persons running the TRIP platform. *Siesby*[67] claims that the intention of the Convention is not to seek a choice of law on behalf of the subjective connections, nevertheless, these connections are relevant as to the choice of law on same level as the objective connections.

b. Closest connection related to air travel

Until now we have discussed the principal rule of the closest connection. This rule is stated in the Art. 4(1) of the Convention. In the Art. 4(2-4) there are special provisions concerning the application of the closest connection method. For contracts concerning air travel, it is the Art. 4(2) that is interesting. The Article states:

> "...Subject to the provisions of paragraph 5 of this Article, it shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of the conclusion of the contract, his habitual residence, or, in the case of body corporate or incorporate, its central

but Norwegian courts found that there under the circumstances were no reasonable justification to decide a case between two Norwegian ship owner according to foreign law [whereafter they applied Norwegian law].

[66] See, Siesby, p.57

[67] See, Siesby, p.73

administration. However, if the contract is entered into in the course of the party's trade or profession, that country shall be the country in which the principal place of business is situated or, where under the terms of the contract the performance is to be effected through a place of business other than the principal place of business, the country in which that other place of business is situated."

Paragraph 5 of this Article states that the paragraph 2 shall be disregarded/not applied if either the characteristic performance cannot be determined or if it appears from the circumstances as a whole that the contract is more closely connected with another country. As for air travel contract, the last part might be interesting. If a airline ticket is purchased on the TRIP platform(English), but concerns a IBERIA flight from Barcelona to Madrid, the closest connection seems to be Spanish. However, according to report on the Convention: "...contracts for the carriage of the passengers remain subject to the general presumption, i.e. that provided for in Article 4(2)...".

Looking back at the Article 4(2) this causes problems. Firstly, the problems concerning consumer protection will be dealt under the respective section of this report. Secondly, the question is whether the responsible for the TRIP platform can be said to "...effect the performance which is characteristic of the contract...". TRIP is, as we have understood only an intermediaire for the airline, but the customers counterpart. And the characteristic performance of the contract is the carriage of passengers. If the court chooses to consider the TRIP platform as the one effecting the characteristic performance of the contract, it will be the place of TRIP's administration that gives the applicable law. If not, it is quite possible that the court will apply the Article 4(1) of the Convention, the closest connection method. Thirdly, the Article 4(2) states that the decision of the closest connection shall take place at the "...time of the conclusion of the contract...". The question is when the conclusion of the contract happens. Several possibilities are present, amongst these the demand of the customer, ordering the ticket, TRIP's response to the first demand or even the confirmation from the airline. Fourthly, the Article says that when the conditions stated are present it is a "presumption" that the applicable law is the one of the TRIP's central administration. The use of "presumption" leaves the impression that there are possibilities in some cases that the general rule of the closest connection might be applied, and not the one stated in Article 4(2).

In this report we have not tried to solve these problems, but only tried to raise the issues we believe might cause problems for the TRIP platform. Therefore, we do not continue any further discussion on Art. 4. As to the other points concerning the Article 4 of the Convention. The other points of Art 4 have no important legal impact on the TRIP platform.

4.2.3.4. The limits of the choice of law

Once an applicable law have been chosen, there is still a question as to the validity of the contract. This question has several aspects. Notably, if there is a binding contract between the parties, followed by the question what law is applicable to the formal validity of the contract. In addition, one have to ask weather the choice of law is acceptable, this question only relates to those situations where the parties have chosen the applicable law themselves. The last

problem relates to the question concerning the limits to mandatory rules. In this part of the report we will try do look a bit deeper into these problems.

a. The question of a binding contract

The TRIP platform is based on an Internet offer, giving the customer the possibility to order tickets and reserve them. Between the customer and TRIP there is a contract binding the parties together. The customer must pay a certain amount of money, while TRIP must deliver the ticket. The question that raises is a what point one can say that the parties have committed themselves to a contract. From a private international law point of view, this might cause problems because not all countries have the same rules concerning the point at where a contract is considered binding. In Norway a contract is considered binding when the accepted response to the offer has come to the knowledge of the one offering. In English law, the contract is binding when the response to the offer is sent. These types of differences might cause problems. Especially for a platform like the one TRIP is intended for, this might be a possible problem. Another aspect of this problem is the process where two parties have negotiated a contract. There can be several offers and negotiations of these. At what point is the contract binding. For contracts made over the Internet, these are possible problems.

The question is whether there is a material validity to the contract. As to this problem, Article 8(1) states:

> "...The existence and validity of a contract, or of any term of a contract, shall be determined by the law which would govern it under this Convention if the contract or term were valid..."

The principal rule can therefore be said to imply the application of either the law chosen in a choice of law clause, or by the law that have the closest connection to the case after Article 4 of the Convention.

For the customer, this might seem a bit strange, because entering the Internet, he can not automatically know where each website is situated. The IP-number of a computer or the name of each website does not always give such information. Therefore, if the general rule of the electronic commerce would be the application of the law of the contract (closest connection/choice of law clause) the customer could risk to end up in a contract he never intended to be binded to. This argument must be seen under the perspective, that it is the website that offers a service. For certain situations, the Convention therefore has an exception to this paragraph, namely Article 8(2):

> "...Nevertheless a party may rely upon the law of the country in which he has his habitual residence to establish that he did not consent if it appears from the circumstances that it would not be responsible to determine the effect of his conduct in accordance with the law specified in the preceding paragraph..."

This implies that in certain situations the customers of TRIP might defend themselves by saying that in accordance to their legal system and contract law, they have not consented to any contract. The question then raises, in what situations the Article 8(2) can be applied. According to the Report on the Convention the word "conduct" covers both action and failure to act. The words "if it appears from the circumstances" have regards to all circumstances of the case, including previous business relationships. The word "a party" can relate to either the offeror or the offeree. According to Allan Phillip[68] the Article relates to persons that are not used to international commerce. Whether all users of the Internet can be considered to not being used to such type of commerce, can therefore be argued. Are solution to this problem is not offered, but both possibilities are present.

b. Formal validity of the contract

On the other hand, all contracts have to have a certain form. If not, they will not be valid. For the TRIP platform, this might cause certain problems. First of as to the formal validity of the contract, and second as to the technical problems.

As to the first problem, this problem is solved by the Article 9 of the Convention. In respectively paragraphs 5 and 6, the questions are about consumer protection and immovable property. Non of these are treated her, as the main question is what law governs a general contract in the context of TRIP.

In paragraph 1, the problem is where all parties are in the same country[69]. Such a problem is thinkable for TRIP, e.g. id TRIP is situated in England and the customer is also situated in England, but the airtravel is with a foreign airline and happening abroad. If this is the case, the formal validity depends on the formal requirements of English law. In paragraph 3, it says that if one of the parties is an agent, it is the place of the agent, and therefore the customer that governs the validity. The latter problem can be thinkable, if TRIP has several sub-branches in different countries.

If the parties are in different countries, according to paragraph 2, it is the law after either Article 3(the parties have made a choice) or Article 4(closest connection) that governs the validity. If this is not satisfactory, the contract is still valid if the validity is satisfactory in one the countries of the parties. This might seem difficult to understand that the contract might be formally valid, even though it not satisfactory in the country of the customer. However, one must not forget that the contract is binding after Article 8, and since it is found that the parties had an intention of forming a contract together, it is the intention of the Convention to try not to find the contract invalid because of formality.

However, all three paragraphs have in common, one interesting point. This is, when a contract is made over the Internet the physical location of the persons behind the contract, might not be the important connecting point as to where they are. One could for instance argue that the contract, if made like an offer on a website with a fill-in form, is actually made on the website, where the server is located. On the other hand, one could also argue that since the

---

[68] See Allan Phillip: *EU-IP(2.udgave), København 1994,*p.169

[69] One has to remember that a case where both parties are in the same country, can still be a problem concerning private international law, because the fulfilled of the contract, can happen abroad.

website and the offer is present at the customer's screen, the contract has in full been completed in the customer's country. An extra argument for the latter solution is that the offeror, by publishing something on the Internet, knows its international aspect, and he, therefore, must suffer the consequences. In addition, paragraph 2 relates to an agent. According to the Report on the Convention and also supported by Morse[70], this covers all sorts of agents, both direct and those without any direct link to the main office. For the Internet offer, one could argue that the website downloaded, represents a sort of agent, especially if it is in English or in the offeree's language. Many websites have today the possibility of supporting several languages, e.g. the website of the EU: www.europe.eu. Hence, the result for an Internet offer could therefore be, regarding Article 9, that the formal validity always follows the country of the offeree. Consequently, this could lead to a difficult situation for the offeror, always trying to adapt to a new country.

As to the technical problems, they are a bit different. And probably should be treated under its own. On the other hand, the report does not give us the space to treat it as a single subject. The problem goes as to the certainty of the parties and the safety of the contract. Electronic commerce is in its beginning. This means that the safety of the Internet, the means of payment, the signatures, the importance of click-wraps, the methods of encryption, the possibilities of firewalls etc. are all elements of electronic commerce. The requirements for a safe transaction are not clear, but they are starting. The is no doubt in our minds that in very few years there will be provisions demanding a minimum level of such technical "security". This will again lead to the question concerning private international law, what countrys "technical" law is applicable to the safety of the contract. Today, we see these questions to be of the same nature as the validity of a electronic contract. It can also be argued that they are both of material and formal validity, implying the use of both Articles 8 and 9.

c. The limits as to the mandatory rules chosen by the parties

Once a law is chosen by the parties another question arises, namely if the court will accept the choice. Not as to, if the choice it self is valid, but if the applicable law chosen is in breach with mandatory rules of lex fori or what the parties normally are entitled to. "Mandatory rules" are described as being the rules of the law of the country which cannot be derogated from by contract. The most common situation where the court might argue that the chosen law can not be applied, concerns consumer contracts in Article 5 of the Convention. The reason behind such rules is to protect the weaker party. The question relating to this problem is discussed in another section of this report. However, there are other questions concerning this choice of law in the contract, namely, outside areas like consumer protection, where there are other mandatory rules.

In Article 7 of the Convention, it is stated:

> "...When applying under this Convention the law of the country, effect may be given to the mandatory rules of the law of another country, with which the situation has a close con-

[70] C.G.J.Morse, *International and Comperative Law Quarterly, Volume 41, London 1992,* p.7. This part actually concerns Article 5 of the Convention, but it explains "agent", which is the same in Article 9.

nection, if and in so far as, under the law of the latter country, those rules must be applies whatever the law applicable to the contract..."

This implies that if a case has close connection to one country, other than the one chosen, either by the parties or as a result of Article 4, the mandatory rules of this country must not be avoided. Article 7 has its similar in different Conventions, like the 1978 Hague Convention on the law applicable to agencies, Article 16.

The question is, what kind of close connection is demanded. According to the Report on the Convention:

"...it is essential that there be a genuine connection with the other country, and that a merely vague connection is not adequate...there would be a genuine connection when the contract is to be performed in that other country or when one party is resident or has his main place of business in that other country..."

As for the TRIP platform, one could therefore argue, that the contract must in all cases take concern versus the mandatory rules of the country of the offeree (customer), the country of the offeror (TRIP), and the country of the destination or departure (where the contract actually is performed). This could then of course lead to a situation of unpredictability. As a result, the last part of Article 7(1) states that in order to give these mandatory rules effect, regard shall be taken as to the nature and purpose and to the consequences of their application or non application. This, of course, limits the application of all mandatory rules.

For electronic commerce, the full application of the Article 7 would lead to a very uncertain situation. Hence, this leads to the conclusion that Article 7 is very wide, but unprecise. Finally, we will therefore try to give some comments as to how some other country have considered or consider the situation of mandatory rules. According to Batiffol[71], a choice of law clause could repress mandatory rules if the law chosen had connection to the case, and the chosen law was not a evasion (fraude á la loi) of the mandatory rules. In English private international law, there are certain limits as to the freedom to chose an applicable law. The choice must be *bona fide and legal*[72], and not against public policy. Furthermore, English law have ask questions concerning; if a unconnected law can be chosen[73] or if a meaningless choice of law clause is valid[74]. These are all just questions that could be taken into account when determining if the choice of law can suppress mandatory rules. We will not take this discussion any further.

[71] See, Siesby, p.79

[72] Ibid., *Vita Food Case*

[73] *Boissevain v Weil*(1949) 1 KB 482 at 491, Lord Denning: "...I do not believe that parties are free to stipulate by what law the validity of their contract is to be determined. Their intention is only one of the factors to be taken into account."

[74] *Compagnie D'Armement Maritime SA v Compagnie Tunisienne de Navigation SA* (1971) AC 572.

Article 7(2) has its origin in the concern to safeguard the rules of the law of the forum, e.g. cartels, competition, consumer protection etc. These rules are mandatory whatever the law applicable to the contract may be.

4.2.4. The choice of law and ordre public in contracts

As stated above, English private international law demands that the choice of law must be bona fide and legal, and not against public policy. In The 1980 Rome Convention, Article 16 states:

> "...The application of a rule of the law of any specified by this Convention may be refused only if such application is manifestly incompatible with the public policy ('ordre public') of the forum..."

Once a law has been chosen as the law applicable to the contract, and the applicable law does not interfere with mandatory rules, the forum might still prohibit the choice of law. This is so-called negative ordre public, i.e. disregard of rules normally applicable. This is only in certain specific cases, and rarely thinkable for contracts in a European perspective. However, it must be mentioned, that shall Article 16 come to use, it is not the choice of law clause that is invalid, but the application of a certain rule of the applicable law that is incompatible with the public policy if the forum. A rule of an applicable law, that does not come to use, can not imply the use of Article 16.

Finally, what is the meaning of public policy? Public policy rules are rules that cannot be compared to mandatory rules of a country. This would be wrong use of the Article. Public policy refers to general social and ethical rules of a country. In certain cases, like for alcohol, the social policy in Norway is to limit the use of alcohol, this contrary to public policies in several central European countries. A contract involving alcohol could, therefore, be prohibited in Norway in the context of Article 16 of the Convention. As for a platform like TRIP, it is very unlikely that the contracts involving European transactions for tickets and reservations would be confronted with Article 16.

4.2.5. . The situation between TRIP, the airline and the customer: airline provisions

One of the problems of the TRIP platform, is how the platform is supposed to function in respect to the guidelines of the airlines. Most airlines gave their own set of rules, or use standard rules. This report has considered two parties at the end of one single contract. Here, it is TRIP selling a ticket and the customer buying the ticket and therefore paying. The airline is linked to TRIP, but does not have a direct contact with the customer. As a consequence, we have not discussed these airline provisions, but only related the discussion to the contract between TRIP and the customer.

As to the airline provisions, these are normally related to standard agreements concerning liability due to loss of life, injury or loss of baggage. If these provisions are valid for the customer depends on the contract between TRIP and the customer. In a choice of law clause, a reference to these sorts of provisions, is just the type of clauses where there is severability, which probably will be accepted by the courts. On the other hand, these airline provisions might be suppressed by mandatory rules. This report does not discuss these provisions any further, as they are not a part of the scope of this report.

4.3. Consumer protection

4.3.1. Introductory remarks

It is likely that a significant proportion of the customers negotiating the services that the TRIP pilots are going to provide will be considered consumers. The term "consumer" is in a juridical context normally defined as a private person who aquires goods or services mainly for his own use and not for resale or use in business[75]. This is, more or less, also the definitions used in the EC Directives concerning consumer protection[76], and the Rome Convention of 1980, see art. 5, 1st paragraph.

If the customer is a consumer, he is normally granted special privileges in legal disputes where the counterpart is a professional. The reason is that the consumer is normally considered the weaker party to the contract, and the governments in Europe have in the latest centuries wanted to place the consumer on a more equal footing to the vendor. As concerning the choice of law, they have seeked to do this by imposing rules which makes it more difficult to deprive a consumer the mandatory rights he normally enjoys within his own country. In the recent council resolution of "The consumer dimension of the information society", the Council of the European Union underlines that the consumers should be able to benefit from the protection afforded by the legislation of their country of habitual residence[77]. In the following we are going to examine whether there already exist instruments within Europe that provides for such special protection of the consumers. The question to be analysed is whether the choice-of-law clause may deprive the consumer of mandatory consumer protection legislation of the state whose law would otherwise be applicable.

However, it should be said that since this report is only considering contracts negotiated between parties both situated within the European Community, it is not very likely that the differences between the consumer protection legislation of two Member States will be significant, hence the legislation concerning consumer protection has been harmonised to a great

---

[75] Bernitz, U: "Consumer protection: aims, methods and trends in Swedish consumer law" in *Scandinavian studies in law (1976), pp 21-22.*

[76] Council Directive relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising, OJ 1984, L 250/17, Counsil Directive to protect the consumer in respect of contracts negotiated away from business premises: OJ 1985, L 372/31 and Council Directive on the protection of consumers in respect of contracts negotiated at a distance (distance selling): OJ 1992, C 156/14.

[77] Council resolution as agreed at the Council of Ministers on 3 November 1998.

extend within the EC[78]. Still some differences may exist, and consequently the questions concerning choice of law will be relevant.

In this survey, we are not going to rise the questions whether the parties have the right to include a choice of law clause to the contract, or whether the clause itself is materially valid. Generally, it may be noted that few restraints exist upon including a choice of law clause, and normally the content of the clause is considered materially valid. We therefore presume in the following that the clause of interest is binding to the contract parties.

4.3.2. Application of national mandatory rules

The central instrument for determining the choice of law within the EC area, is the Rome Convention of 1980[79]. The starting point is that a contract shall be governed by "the law chosen by the parties", cf. Art. 3. As the consumer normally is the weaker party of the contract, this can make it easy for the professional part to deprive the consumer of the special consumer protection often offered by national mandatory rules. Even if national mandatory rules cannot be derogated from by contract, they may be circumvented if one choose another country's law to govern the contract. Consequently, if the law chosen offers little or none consumer protection the consumer could find himself in trouble. The consumer will often be in a position that makes it difficult for him to protest against a clause like this.

To seek to prevent situations like these, special privileges are given the consumer in art. 5(2), which makes mandatory consumer protection rules of the consumer's country of residence applicable in situations where the consumer can reasonably expect them to apply.

The article provides that a "a choice of law made by the parties shall not [deprive] the consumer of the protection afforded to him by the mandatory rules of the law of the country in which he has his habitual residence." As we can see, the provision does not prevent the parties from choosing another law than that one of the consumer's country. However, the chosen law must not place the consumer in a poorer position than would have been the case if his home country's law where to be applied. The consumer may therefore always enjoy the special consumer rights he is granted within his own jurisdiction.

The provision is subject to three alternative craters. Here only the first will be examined as the two others are not particular relevant in our context. The first criteria requires that the conclusion of the contract was preceded by a general advertisement or specific invitation addressed to the consumer, or in the country he reside, and that he took all the steps necessary on his part to conclude the contract in the same country.

An important exception to art. 5 (2) is set out by art. 5 (4) b. This provision holds that even if conditions of the former paragraph is fulfilled, the consumer will not benefit from the mandatory rules of his law if the contract is for the supply of services which are to be supplied the consumer exclusively in an other country than the consumer's.

---

[78] The most important instruments being the Council Directive 93/13/EEC on unfair terms in consumer contracts and the European Parliament and Council Directive 97/7/EC on the protection of consumers in respect of distance contracts.

[79] EC Convention on the Law Applicable to Contractual Obligations (Rome 1980).

Whether a contract negotiated on the Internet will be caught by art. 5 of the Rome Convention, is the issue to be examined in the following.

4.3.2.1. "Specific invitation" addressed to the consumer, art 5(2), 1st alternative.

Clearly, if the service supplier chooses to promote his products by sending offers and prompts via e-mail, this will be considered a "specific invitation" and consequently caught by art. 5(2)[80]. That the offer is sent by electronic means instead of traditional mailing systems is irrelevant.

4.3.2.2. Previous advertising, art 5(2), 1st alternative.

Normally when speaking of advertising, one refer to advertising in more traditional media like the press, radio, television or cinema. The crucial point seems to be the location of the advertising; whether it takes place *in the country* of the consumers habitual residence or not. The essential point is where the advertisement was perceived, not the location from where it was initiated. Applying these principles in a digital environment obviously may cause problems, given that no national boarders exist on the Internet. When one advertises products or services on a web page, the advertisement is factually located on the server which contains the web page. This would imply that if the server in question is located in a country other than the consumer's, the situation falls outside the scope of art. 5(2). It is the consumer himself that have imported the advertisement to his country by requesting the web page. This situation has similarities with a consumer travelling abroad who gets hold of a magazine containing advertisement, whereby he when returning to his home country subsequently accept one of the offers in the magazine for example by telephone or letter. It is clear that situations like this last mentioned falls outside the scope of art. 5(2), due to the fact that a) the supplier could not reasonably have foreseen that he was dealing with a consumer situated in another country than that where the magazine was sold, and b) the consumer himself would not have any just expectations that he could rely on the consumer protection rules of his home country to apply. However, these arguments are weakened when it comes to advertising on the Internet. This is mainly because it will always be predictable for the service provider that the advertisement could come to the attention of consumers situated in another country, even if he primarily intends the web page to be read by consumers of certain countries. Furthermore it will not be that obvious to the consumer that he can not rely on his own country's consumer protection law, since he at the moment he accesses the advertisement after all is being in his home country. It is therefore probable that we in future cases will experience that the courts seek to avoid following the wording of the paragraph strictly, but instead chooses to put more weight

[80] The other solution though could be argued if the server to which the e-mail is sent is situated in another country than that of the end user who downloads the e-mail to his personal pc. This situation has little practical interest, and will not be followed any further.

on the purposes of the provision. In this is the case, one might end up with a situation where practically all countries jurisdictions could be potentially applicable to consumer contracts negotiated on the Internet. One way to avoid this situation, is choosing only to conclude contracts with consumers situated within a certain area.

4.3.2.3. Steps taken in the country of residence, art. 5(2), 1st alternative

For the rules in art. 5 to apply, it is required that the consumer took "all the steps necessary on his part for the conclusion of the contract" in his own country. It is the factual, not the legal steps that are the concern of the provision. On the Internet there are two ways for the consumer to place his acceptance of the offer. Either by email or by filling in and posting an order form directly onto the supplier's web server. The former situation is comparable to circumstances where a consumer accepts an offer by posting an ordinary mail. This clearly must be regarded as all the necessary steps were concluded in the consumer's country. When it comes to the latter situation, this should not be treated any different. The location of the server where the acceptance form is situated is fortuitous, and the means of communication should not be crucial. The relevant steps when it comes to the acceptance of an offer on the Internet, must be the typing on the keyboard or posting the email or form by pressing the appropriate button.

Difficulties may occur when the consumer electronically accepts an offer while he is travelling abroad or similar. However, these situations are not that practical and will not be followed further in this survey.

Place where electronic services are to be supplied, art. 5(4)B

The pilots are going to sell services, not tangibles. Therefore the provisions of art. 5(4) b may apply provided that the service is considered to be supplied to the consumer "exclusively in a country other than that in which he has his habitual residence". It is possible to determine quite easy where physical services are to be rendered, e.g. train travels, shoe shining and similar. By contrast it can be hard to determine the place where a non-physical service is to be rendered. As a point of departure, it seems difficult not to assert that the location of the service is the actual location of the used resource. This would mean that the service must be considered to be supplied to the consumer exclusively outside his home country given that the server is located in another country. However, it seems unlikely that courts will hold as the determinant criteria the location of the server from where the service is supplied[81]. This is because it would be very easy for the supplier of the service to shop around for the most appropriate law simply by providing the service from a server located in a country with favourable legislation. It is therefore likely that the relevant connecting criteria will be to determine in which country the supplier of the service is established[82]. The place of establishment

[81] In its proposal for a directive on certain legal aspects of electronic commerce, the European Commission generally excludes the location of the technical equipment used as a relevant connecting criteria, see "Proposal for a European Parliament and Council Directive on certain legal aspects of Electronic Commerce in the Internal Market".

[82] This is also the general approach taken in the Proposal for a directive on electronic commerce, mentioned in the former footnote.

probably would be assessed in accordance with the EC-courts statements concerning the term "establishment" used in the EC-Directive on the protection of personal data[83]. This would mean that if the supplier of the service is situated in a country different from that of the consumer, the consumer would not enjoy the special rights he is granted after the Rome Convention art. 5.

However, it is still not sure if such a solution is going to be adapted to the problem in future cases. This is mainly because that such a result seems to be unsatisfactory from a consumer-right perspective. It would mean that it would be easy for service providers on the Internet to evade the stronger protection provided to consumers in many countries, given that many of the services provided on the Internet must be considered non-physical. The reason to operate with an exception when the service is going to be rendered exclusively outside the country where the consumers reside, is mainly because that the contract is in these circumstances considered more closely connected with the state in which the service is going to be supplied. The argument is then that the consumer can not reasonably expect the consumer protection law of his own country to be applied in derogation from the general rules of art. 3 and 4[84]. It is not that clear why a consumer should not reasonably expect his own national consumer protection law to apply when contracting for example mediating services on the Internet supplied from a service provider established in another country.. The situation here differs from the examples mentioned in the commentaries to article 5(4); accommodation in a hotel situated abroad, or a participating in a language course abroad. In these two mentioned examples, the consumer typically stays abroad at the same time as the service is rendered. By contrast, when the service is being rendered on the Internet for example in the form of a mediating service, the consumer is likely to be placed on his office chair or his sofa in his home country when receiving the service. It should therefore not be taken for granted that that a situation like those here mentioned automatically will lead to the derogation from the principles laid down in art. 5(2).

When it comes to contracts concerning the provision for a "combination of travel and accommodation" – so called package tours – special provisions are given in art. 5(5). This paragraph provides that even if the conditions of the 4th paragraph are fulfilled, still the principles laid down in art. 5(2) will apply. This means that even if both the travel and the accommodation is rendered exclusively abroad, still the consumer will enjoy the protection offered by the consumer protection law of his home country.

4.3.2.4 The professional party could not reasonably have foreseen that he was dealing with a consumer.

In the commentaries on the article it is stated that situations where the professional party did not reasonably have any reason to believe that he was dealing with a consumer even if he was taking all the circumstances into account, the situation falls outside the scope of art. 5. This opinion may have great influence on services offered on the Internet, because it will be

[83] See the ECLIP report concerning data protection for further information.

[84] Report on the Convention on the law applicable to contractual obligations by Mario Giuliano, Professor, University of Milan, and Paul Lagarde, Professor, University of Paris.

difficult for the service provider to know for certain whether he is dealing with a consumer or not, given the anonymity the buyer may operate under. The subject of the agreement may indicate whether one deals with a consumer or not, as for example when one is offering products or services that a typical consumer would not have bought. However, when it comes to selling travels, the products itself cannot always give good clues for determining what kind of customers are likely to buy them. One might therefore very well find oneself in a situation where the service provider could not reasonably have foreseen that he was dealing with a consumer. If that is the case, the special provisions given under art. 5 to protect the consumer's interest would not apply, and the consumer might find himself in a situation where the consumer protection he is offered is inferior compared to the mandatory rules of his home country.

4.3.3. Application of international mandatory rules

Given that the provisions of art. 5 does not apply to the case, it will not be possible to give effect to national mandatory rules. However, it will in some cases still be possible to enforce international mandatory rules concerning the protection of consumers irrespectively of the law chosen by the parties. In article 7 of the Rome Convention rules are given for the application of so-called international (or conflict-type) mandatory rules. By contrast to the national mandatory rules which have been the subject above, the international mandatory rules purport to be applicable even if the parties have chosen another law. As a starting point it is therefore impossible to circumvent these types of mandatory rules either by contract or choice of law.

If these types of mandatory rules exist in the forum country, they shall apply to the contact "irrespective of the law otherwise applicable to the contract", c.f. art. 7(2). However, also international mandatory rules of *another country* than the forum country may be applied under certain conditions, c.f. art. 7(1). The condition is firstly that "the situation has a close connection" to that country. It is also said that regard shall be had to the rules nature and purpose and to the consequences of their application or non-application, in considering whether to give effect to these mandatory rules. The provision has been criticised for making it very difficult to predict which law will apply in a potential future case. An example may illustrate this: If the parties have chosen Italian law to govern the contract, and the forum country is France, it will be possible that the French court will find that English international mandatory rules are applicable to the case.

To be able to predict, in some way, which international rules that may apply, one have to determine with which countries the situation has a close connection. In the commentaries to art. 7 it is said that it is essential that there is a genuine connection with the other country, and that a merely vague connection is not adequate. For example, it is said, there would be a genuine connection "when the contract is to be performed in that other country or when one party is resident or has his main place of business in that other country". The connection in question must exist between the contract as a whole and the law of a country other than that to which the contract is submitted.

4.3.4. Ordre public

If the application of a foreign law in an actual case would give a result which would have been manifestly incompatible with the public policy ("ordre public") of the forum where the case is being adjudicated, the application of that specific rule may be refused or modified. This common principle of private international law is expressed in art. 16 of the Rome Convention. However, strong reasons have to be adduced before the provision can be applied, c.f. the expression "manifestly incompatible". It is clearly not sufficient that the result from applying the foreign rule would be another than if the national mandatory rules of the forum were to be applied. Within the EC it is therefore very unlikely that a court will hold that the application of consumer protection legislation of another Member State will give a result that is manifestly incompatible with the public policy of the forum country. This because, the consumer protection legislation, as mentioned above, is to a large degree co-ordinated through the different directives issued on the subject of consumer protection[85].

4.4. Liability on the basis of loss suffered due to misleading information

4.4.1. Introduction

Liability may be both criminal and civil, and both forms could be the result of loss suffered due to misleading information. This report will not discuss criminal liability.

Misleading information is in many ways just a part of advertising and can occur through the advertising on the Internet, i.e. the information on the website of TRIP.

What kind of misleading information is this? First of all we consider this to be a prolongation of the commercial transaction. This implies that the misleading information has lead to an economical loss by the customers of TRIP. Third party-situations are not discussed in this report.[86]

The kind of loss due to misleading information is primarily caused by the merchandise or product delivered by TRIP. In the context of this report we will not discuss the liability questions solved by a potential contract. It must be mentioned, however, that if there were a contract[87] between the seller (TRIP) and a customer, there would be certain limitations for what

[85] The most important being the Council Directive 93/13/EEC on unfair terms in consumer contracts and the European Parliament and Council Directive 97/7/EC on the protection of consumers in respect of distance contracts.

[86] Typical situations where Internet-surfers find information on the Internet and act on behalf of this, without doing anything more than looking at the web-site. Another third party is the one who's loss is based on wrongful information about him on this web-site, i.e. «Mr. A sells products fare worse than ours».

[87] The Rome Convention states that the parties have full autonomy to make a choice of law, cf. art 2. This could again raise the question whether there is a binding contract between the parties, if this contract is due to a web wrap. We do not pursuit this question.

can be regulated on this contract. For consumer purchases notably, mandatory rules are guaranteed by the Rome Convention art. 5(2).[88]

Finally this would mean that the loss a customer may suffer due to misleading information, is the type which is not regulated in a contract. It can be the information the customer has trusted when purchasing the ticket. For example if the ticket that the customer has purchased does not give him certain rights on board the flight,as the customer was promised. The customer will then have to purchase these services on his own. Another example would be, if the issued ticket does not correspond with a certain flight, or the flight is cancelled, and the customer does not get automatically a new ticket and has to buy one instead. In these types of situations, there could be a question of loss suffered due to misleading information. It may also be information misleading the customer not to take advantage of a favourable offer.

In the following we will pursue the choice of law that governs the liability, but first we will look at the regulation, or the lack thereof.

4.4.2. Regulations and the lack of these

Inside Europe the EU has issued several Council Directives dealing with misleading information and other problems like protection of consumers' interest.

This is notably the Council Directive 84/450/EEC of 10 September 1984 relating to the approximation of the laws, regulations and administrative provisions of the Member States concerning misleading advertising. This Directive gives a definition of misleading information in art.2(2):

> '...means any advertising which in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect their economic behaviour or which for those reasons, injures or is likely to injure a competitor ...'

This would mean that the misleading information we are discussing under this point of the report is similar to the term ''misleading advertising'' in the Directive. Unfortunately this Directive does not give any guidance as to what the choice of law should be in the context of loss suffered due to this type of advertising, even though it sets a standard for what the bottom line of misleading information cannot be.

Furthermore, there are Directives, which deal with the protection of consumers. Here we can mention the Council Directive 92/28/EEC on the advertising of medical products for human use, the Council Directive 93/13/EEC on unfair terms in consumer contracts, and even the Directive 97/7/EC of the European Parliament and of the Council on the protection of consumers in respect of distance contracts. Again, these Directives only set a certain standard for consumers, and they do not give a choice of law as to the liability when breaking these rules.

---

[88] For a more extensive discussion, cf J. Benno: *Consumer purchases through telecommunications in Europe,* Complex 4/93 Tano (Oslo 1993).

In the Directive 98/27/EC of the European Parliament and of the Council on injunctions for the protection of consumers' interests, it is stated in art. 2(2) that:

> '... This Directive shall be without prejudice to the rules of private international law, with respect to the applicable law, thus leading normally to the application of either the law of the Member State where the infringement originated or the law of the Member State where the infringement has its effect ...'

As to what an infringement shall mean, this is stated in art. 1(2) dealing with the scope of this Directive:

> '...For the purpose of this Directive, an infringement shall mean any act contrary to the Directives listed in the Annex as transposed into the internal legal order of the Member States which harms the collective interests referred to in paragraph 1 ...'

The Directives of the Annex include the Directives listed above.

From this point there are several conclusions that can be made. The first conclusion is that in spite of the harmonisation inside the EU/EEA-system, the field of private international law still has a place. All cases addressing infringements in a private context, must first be solved through a private international law argument. The second conclusion suggests that the choice of law rule applicable to which law governs the liability question, is either the law of the Member State where the loss was originated or the law of the Member State where the infringement has its effect.[89]

As for the Directives mentioned above now, the conclusion must be that they might imply the application of a certain rule or rules, but these rules are not clear enough to suggest a choice of law for loss suffered due to misleading information. The only clear conclusion, from the Directive on injunctions for the protection of consumers' interests, must therefore be that private international law governs cases where there has to be a choice between several laws of the EU/EEA-community. This again brings us to the basic rules of private international law of liability outside of contract.

4.4.3. The basic rule of private international law of liability outside of contract: *lex loci delicti*

As we saw in sect 2.7, there are several solutions to an international dispute. Everything from the domicile of the buyer or seller, to the use of *lex fori* is available. In contrast to this

[89] It could though be argued that the choice of law process should go through two steps, one choosing the law to govern if there has occurred a loss(like if it where an infringement), and the second choosing the law to govern the liability. We believe that this is pointless, because both points still would have the same choice of law-rule.

are the solutions concerning liability and infringements outside of contract. In private international law the basic solution for liability outside contractual obligations is the rule of *lex loci delicti*[90] – the law of the place of damage. This is normally quite clear in the field of physical damage, and the damage will mainly be located at only one place. For example two buses collide in country A. The busses do not come from this country, nor do they come from the same country. The law to govern the liability suit is the law of the country where the damage happened, i.e. country A.

The question is therefore whether the rule of *lex loci delicti* is applicable to solve liability due to misleading information in the context of a commercial transaction on the Internet. Looking at the problem there are two potential solutions: The law of the country where the damage has its origin, or the law of the country where the damage has occurred. These solutions have been outlined by the Directive 98/27/EC on injunctions for the protection of consumers' interests' art. 2(2). For a problem of loss due to misleading information, either the law of the country of the web-site[91] or the law of the country where the loss is suffered would apply. Both these solutions can have different outcomes.

The law of the web-site could be a solution, considering that the loss is due to the misleading information on the homepage. This homepage is then the natural source of the loss. Unfortunately it would be to easy for the web-owner to locate the server in a country with non-existing liability rules. In other words, the law of the web-site, as a simple rule, could lead to forum shopping.[92] Therefore the nearest solution is to apply the law of the web-site as the law of the country where the establishment operating the web-site is located. Not only would this follow the Directive 95/46/EC on Data Protection, but this would also correspond more with the intentions of the traditional rule of *lex loci delicti*. There are strong arguments for such a solution, mainly the predictability for all the parties. For the customer suing, this would also mean that his opponent has stable location. For the seller ('opponent') this implies the advantage of being always sued according to one set of rules. On the contrary this can also lead to an unfair situation; since the seller has accepted to sell on the Internet and thereby to a variety of countries, the liability should follow the place where the damage or loss is suffered.

Choosing the law of the country where the loss is suffered, is not as clear as it might seem, although the loss is clearly related to the person[93] that has purchased from the web-site in question. Unfortunately the ''loss'' can be related to several places. The places in question could be the domicile of the person that has suffered the loss, the place where the loss actually took place[94] or it could be the one the person's citizenship. Choosing the place where the loss actually took place, could here also mean the place where the economic loss took place or where the damage that caused the loss took place. Without going any further in this discussion, and without trying to solve a problem any court has decided, we would suggest the law of the country of the domicile of the person that has suffered the loss.

---

90 See Helge J. Thue: *Norsk International obligasjonsrett, erstatning utenfor kontraktsforhold* (1986) UiO, Stensilserie nr.111.

91 The location of the web-site would here, in its simplicity, mean where the server that contains the web-site is situated.

92 Forum shopping refers to the situation where the party or the parties search for the law of a country that suits them best, and thereby they escape the natural court.

93 Could be legal or physical.

94 Which is not the one of the domicile or citizenship.

Trying to determine whether the *lex loci delicti*-rule of private international law is applicable to the problem raised by loss due to misleading information, causes many difficulties, mainly because this cannot be anything more than an assumption. On the other hand the rule of *lex loci delicti* is still a part of private international law. The best solution to this rule would, in our opinion, then be to make the choice of law according to the country of the establishment behind the web-site.

Unfortunately the rule of *lex loci delicti* is not the only candidate. The simple choice of law rule based on the geographical relation seems to have certain insufficiency. Some courts would seem in favour of applying *lex fori*. Inside the EU/EEA, where the Lugano and Brussels Conventions determines the jurisdiction,[95] and where the geographical relation between the loss and the jurisdiction has placed the lawsuit in one court, it is not unlikely that the court will apply *lex fori*. This would follow the unfortunate ''homeward trend''. However the latter solution is not acceptable in the context of private international law.

Finally another suggested solution to these problems is, the so-called 'principle of closest connection'. The closest connection is found by considering all circumstances of the transaction which may serve as connecting elements, weighing them together and then determining where the contract has its natural centre of gravity,[96] i.e. the closest connection. The connecting elements will then be all the elements mentioned above; from the place of the web-site, the establishment behind the web-site, the country of the buyer, the language of the web-site to elements like where the loss was suffered. This method has a certain flexibility, which is lacking in the other solutions. On the other hand, this method has a large portion of unpredictability. This is why the method has not been fully accepted. Finally it must be said that this solution has been adopted by the 1980 Rome Convention on the law applicable to contractual obligations, cf. art 4(1) on applicable law in absence of choice:

> ''To the extent that the law applicable to the contract has not been chosen in accordance with Article 3, the contract shall be governed by the law of the country with which it is most closely connected...''

If a contract between two parties does not have a choice of law-clause, the solution is the method of the closest connection. This method has also been adopted by the courts, but one could argue that they apply this in cases where the basic rule of private international law does not correspond with their ideas. However there is one leading Norwegian case to illustrate this method. Bing has written in relationship to this matter:

> ''In Norwegian law, there is a famous case of two Norwegian ships colliding in the Mouth of Tyne, and where there was a difference between the maritime law of England and Norway with respect to the liability. Here there was no doubt that the 'injury' took place in British territory, but Norwegian courts found that there under the circumstances were no reasonable justification to decide a case between two Norwegian ship owner according to

[95] See Sect 3.2.

[96] Term first used by C.F. Savigny.

foreign law [whereafter they applied Norwegian law]. The names of the two ships were Irma and Mignon, and the Principe of the closest connection has in Norwegian theory survived as the Irma-Mignon formula''[97].

We have explored the different solutions to the question of what rules could be applied to make a choice of law as to liability. As to drawing a conclusion we find this to be a matter for the reader, and not for us. Though we suggest that the solution should be the one that gives both parties in a lawsuit certain predictability.

4.4.4. The limitations of the choice of law

As already stated in previous parts of this report, the choice of law might conflict with the *ordre public* of the court. It is quite possible that the large amounts of compensation damages given in the USA, will not be given in a European court if the choice of law happens to be American law. In a lower Norwegian court[98] in 1985 there was a liability law-suit against a Norwegian. The choice of law was the Austrian law. On the basis of some sort of *ordre public* argument, the court decided to use the Norwegian limitation rule of 3 years for determining whether damages could be claimed, and not the Austrian limitation rule of 30 years.

4.5. Advertising and choice of law

It is suggested above that the execution of advertisement legislation is part of public law. It is an acknowledged principle that a national court as a point of departure never shall apply foreign law when judging cases of public matters. The general rule therefore is that when it comes to public law, the jurisdiction is not governed by the ordinary collision norms of private international law, whereas it is left for each of the country's practical possibilities to apply their own legislation and determine which law is applicable. Typically possibilities of applying national law will exist if the court has been found competent to adjudicate, see above.

Exceptions from the general rule will principally only take place in cases where international agreements form a different solution, and the state of the court is a party to the agreement. The question therefore becomes whether there are international agreements in Europe which regulate the questions of choice of law concerning advertisement on the Internet.

For the time being, no such agreement exists which regulates the problem directly. However there are two EC-Directives and one European Council Convention[99] concerning the

---

97 Rt. 1923 s. 59

98 Appelate Court Decision (Eidsivating lagmannsrett, RG 1985 s 778).

99 "The Satellite and Cable Directive": Council Directive 3.10.1989 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities (89/552/EEC OJ 17.10.1989 298:25), "The Broadcasting Directive": Council directive of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities (89/552/EEC OJ 17.10.1989

questions of choice of law that concerns cross-border *broadcasting*. Advertising is one of the issues included.

The Directives and the Convention contain the principle that the lawfulness of a broadcast shall be assessed in accordance with the national legislation laid down in the country from where the broadcast originates, which in most cases will imply the country where the seat of the broadcasting company is situated. Given that the broadcasted commercial is in accordance with the advertisement legislation in the country from where the broadcast originates, one will normally not be allowed to restrain the retransmission of the broadcast in neighbouring countries, under the conditions that the contents of the broadcast violate their national rules.

> At least what concerns The Broadcasting Directive, this is not more than a starting point, see the decisions of the EC-court C-35/95 and C-36/95. In these cases it is, under certain circumstances, opened for the application of national law in situations like the one mentioned above. This is mostly due to the fact that the main purpose of the Directive is to oblige the parties not to restrict the retransmission of broadcast originating from other member states, whereas it does not necessarily address the right of the inhabitants to pursue their civil rights. Thus, one might say that even if the principle of "the country of origin" were to be applied to advertisement on the Internet, one could not be assured that the principle would apply under every circumstance.

The question becomes whether the principle of the choice of law laid down in the three mentioned instruments also should apply an advertisement on the Internet. One might adduce good reasons for that this should be the case. To apply the principle of "the country of origin" will simplify determining with which law the service providers will comply. This is because they will only have to consider the advertisement legislation of one country, instead of having to deal with the legislation in practically every jurisdiction of the world. Principles of equality may also be adduced for the support of applying the principle, as it might be inconsistent to let the choice of media in which the commercial is distributed determine the lawfulness of the content. The fact that cable television network may allow connection to the Internet by so called "cable modems", and that the differences from the Internet therefore becomes more subtle, also favours use of the same principles for the Internet as for advertising transmitted through the cable net.

The EC Commission has recently issued a proposal for a directive on certain legal aspects of electronic commerce[100]. The general approach here taken is the same as in the instruments mentioned above, namely applying the principle of country of origin. As a starting point, the principle shall apply to all sorts of *information society services*. Information society services are defined in the same way as in the art. 1(2) of Directive 98/34/EC, as "any service, that is to say, any service normally provided for renumeration, at a distance, by electronic means and at the individual request of a recipient of services". The service provider has to operate his business in accordance with the national legislation of the country where he is "established"[101].

298:25) as amended by the European Parliament and Council Directive 97/36/EC of 30.6.1997, and the European Convention on Transfrontier Television.

[100] Proposal for a European Parliament and Council Directive on certain Legal Aspects of Electronic Commerce in the Internal Market.

[101] The term "established" shall be understood in accordance with the judgment C-221/89 [1991], which sets out a qualitative criteria concerning the actual nature and stability of the economic activity, rather than formal criteria like the location of technical equipment used.

If he so does, other member states may not restrict his freedom to provide his services across the boarders. However, it is still too early to say whether the principle laid down in the proposal, will reach broad consensus within the EC or not. As a consequence, it is still unsure how much weight one should put on the Commission's statements. Accordingly it still not clear whether the courts will apply the principle of country of origin or not in future cases.

This already follows from the general principle, which states that a court always shall apply its own national law in matters concerning public law. It is presumed here that there will have to be strong reasons to deviate from this principle. Since no regulation that may provide for clear answers is in force, it is doubtful whether such strong reasons exist at the time being. As for the regulation in force concerning broadcasting, it cannot necessarily be assumed that the provisions that are formed for the purpose of regulating television broadcasts have taken into consideration the necessary arguments to provide good solutions when applied on other types of media. One must also bear in mind the differences, which exist according to how the transmission of the advertisement takes place in the different types of media. While the broadcasting of a commercial inevitably will have to be considered an active action, it is not that obvious to argue the same when advertising on the Internet.

An additional remark is that the high costs involved with marketing products through television commercials will prevent the smallest and often less serious companies to utilise this medium for the advertisement of their products. It is likely that serious organisations to a greater extent will have an incentive to operate within the limits of normal decency. It may therefore be assumed that legal disputes concerning the contents of a commercial will not occur with the same frequency for television commercials as for advertising on the Internet, where the smaller cost implies that also less serious service providers will be able to market their products or services.

A final remark is that the *forum* country will be inclined to apply their own national law to adjudicate the legal disputes (*the homeward trend*).

Consequently, it is doubtful whether the Directives and the Convention will be applied by the courts, in the sense that the principle of "the country of origin" will apply also on advertisement on the Internet. Most likely, the courts will follow the general principle as mentioned above and apply their own national law[102]. This might be another story if the directive proposed by the Commission concerning electronic commerce comes into force. For that, one will have to wait and see.

4.6. Intellectual property right[103]

[102] However, the application of national law will require that the provisions are applicable on advertising on the Internet. This will in some cases be doubtful, see above.

[103] This chapter is based upon Jon Bing "The identification of applicable law and liability with regard to the use of protected material in the digital context1"

4.6.1 Introduction

TRIPS will probably make use of material protected by copyright law when establishing a web-site. Also, the web page might in itself be considered as protected by copyright law.

In this chapter we are going to deal with the problem of determining which country's law that governs the question of a copyright infringement has taken place. Also, there will be examined, rather briefly, which country's law that eventually will be applied for determining the liability of the copyright infringer. Time will not allow us to consider the choice of law questions which concerns other types of intellectual property right, e.g. the right to domain names, and patents. As a consequence, only the choice of law questions concerning copyright legislation will be examined.

4.6.2 Which country's law applies for determining whether an infringement has taken place?

The most important international instruments which regulates intellectual property right issues, are the Berne Convention (Paris Act) of 1886, the Rome Convention of 1961 and the TRIPS agreement. They all do lay down a rule of national treatment also referred to as the territorial principle. This means that the laws of a State relating to copyright are generally concerned only with actions committed in the State itself.

For this reason one will have to consider in which country the assumed unlawful action is committed, and thereafter apply this country's legislation for the assessment of whether a copyright-infringement has taken place or not.

If the action in question has been committed in "the real world", for example in the form of the photocopying of a book, or a bootleg recording of a concert, it will be simple to pinpoint the action to a specific country. The same applies if a person encounters a web page containing copyrighted material, and prints the material out on his own printer, saves it on a diskette, etc. In all this cases, a copy has been made, and there arise no problems with determining in which country the copying has taken place.

However, problems with connecting an action to a specific country do arise, when the action is not committed within a physical, but rather a digital environment. What kinds of criteria shall then be applied to pinpoint the action in question to a specific country?

For the time being there are no existence of international instruments which provides for clear regulations with respect to the interlegal issues of the computerised information service. Nevertheless, there do exist international instruments, which provides for a regulation on the interlegal issues in other fields. These instruments address the interlegal questions that may follow when information transmitted electronically is crossing boarders. As copyrighted ma-

terial on the Internet can be considered as information[104], the solutions formed in these instruments also may form guidelines for the question that we are here dealing with.

Transfrontier broadcasting is one of the areas where regulations exist. Here we find two EC-Directives and one Council Convention[105] concerning, amongst other, the criterions for pinpointing the relevant action to a specific country. Such criterions also are laid down in the EC Data protection directive[106] for interlegal questions concerning *data protection*. In this report, an examination of what the specific contents of the criteria are will not be undertaken[107], but we will only try to summarise what the instruments various attempts are.

In the regulations mentioned, there can be identified three types of criteria relating a certain action to a specific country:

1) Decisions by the public administration
2) Technical equipment
3) Persons, actors, providers etc.

The former criterion *decisions by the public administration* is functioning quite well in the area of regulating satellite broadcast activities, since the public administration is exercising public authority in licensing frequency capacity. By contrast, a criterion based upon decisions by the public administration is not that well suited when it comes to the regulation of intellectual property rights. This is because the creator of a intellectual work benefits from protection under the Bern Convention independent of whether he has registered a copyright for his work or not. Hence, public administration has little influence when it comes to copyright law, and it would be difficult to identify any such decisions that could be a criterion to relate the issue to a certain country.

As concerning the use of *technical equipment* as a connecting factor, this would seem like an easy way to relate the action to a country. This is because the geographical location of the equipment may easily be determined. However, concerning the great ease of routing the stream of signals, placing them on equipment located in the territory of an other jurisdiction, this may not be such a good solution after all. It would make it very easy to shop around for an appropriate *lex causae,* so-called *forum shopping*, which clearly is not desirable. Anyway, it should be noted that to consider the location of the equipment, in which the relevant action is committed as a connecting criterion, seems to be in accordance with the wording of the Berne-and Rome Conventions and the TRIPS agreement. As mentioned, these instruments hold as the relevant criteria in which country the action was *physically* committed, e.g. in which country the book was distributed. The wording of these international agreements there-

[104] Information roughly may be defined as conveying data in a way which it makes sense to a person.

[105] "The Satellite and Cable Directive": Council Directive 3.10.1989 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities (89/552/EEC OJ 17.10.1989 298:25), "The Broadcasting Directive": Council directive of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities (89/552/EEC OJ 17.10.1989 298:25) as amended by the European Parliament and Council Directive 97/36/EC of 30.6.1997, and the European Convention on Transfrontier Television.

[106] Directive on data protection (Directive 95/46/EC)

[107] For more information, see the article referred to in the footnote of this chapters heading.

fore forms strong arguments for acknowledging the location of the technical equipment, which actually contains the protected work in question as a relevant connecting criterion. This is also an approach taken by many authors[108]. Nevertheless there are many authors[109] that put more weight on the negative factors of operating with such a criterion. What future judgements will lie down as the solution still has to be seen. In our opinion one should avoid to use the location of equipment as relevant connecting factors.

Then it would be better to go for the last types of criterion, namely *persons, actors, providers etc.* These may be related to a certain country by different ties. Typically these ties will be in the form of citizenship, domicile and habitual residence.

In our context, it may be argued that the use of *citizenship* as a criterion may not be appropriate. This mainly because of the great ease it is to move between different countries within Europe. It would be easy for a person to operate permanently for a country different from his country of citizenship. Also it might easily introduce numerous *lex causae* for the protected material in operations otherwise contained within the legal framework of the same jurisdiction.

Something similar can be said for *domicile*, though more closely related to the factual situation of the person, a person for study or work may be outside the country of domicile for prolonged periods. For legal persons, domicile would correspond to the seat of their organisations.

The third possibility would be *habitual residence*, which is mainly a factual criterion – where the person actually operates (with the exception of incidental travels abroad etc.)

If one choose these last types of criterion, it will be far more difficult for Internet providers etc. to shop around for the most appropriate law, i.e. with placing the content on servers located in countries which offer less protection for copyrighted material. Instead of looking at the equipment itself, one will look at the person who is controlling/responsible of the content of the equipment. Imagine for example that a person who has his habitual residence in England, places English official documents on a server in France which is operated by a French host provider.

Official documents are protected in England under the Crown Copyright Act, whereas they are not protected under French law. Nevertheless, this will be seen as a matter of English law, since the person responsible for placing the documents on the Internet has his habitual residence in England. The result will be that the action in question is considered an infringement.

Again it must be said, that it is unsure which connection criterion the courts will choose in future cases. It is even likely that one might experience national differences with tackling the problem. Accordingly, to secure oneself from being convicted for copyright infringments in a future legal dispute, one should try to operate the business within the limits of the law in both the countries where the technical equipment is installed, and the country where the persons, actors, providers etc. in question have their habitual residence, domicile or citizenship.

4.6.3 The principle of "country of origin"

[108] See for example Peter Schøning and Joachim Benno.

[109] For example Jon Bing

Within the EC area it seems to be a tendency for legislation concerning electronically signals that crosses boarders towards that the lawfulness of an action shall be assessed in accordance with the national legislation laid down in the country where the transmission of the signals originates from. Such provisions are for example laid down in the directives and convention above mentioned. Given that the program (or similar) broadcasted is in accordance with the legislation in the country where the broadcast originates from, one will normally not be allowed to restrain the retransmission of the broadcast in neighbouring countries, under the conditions that the contents of the broadcast violate their national rules. This principle is often referred to as the principle of "country of origin". The principle has its advantage in that the persons that wants to transmit material across boarders, will only need to behave in accordance with one country's legal system, instead of potentially hundreds.

It may be argued that the tendency to *convergence*[110] implies that it will be difficult to maintain separate regulating regimes that are media specific, and that one accordingly should adopt the same solution for protected material on the Internet. However, this is more problematical than it would seem at the first glance.

If the principle was to be transferred to copyrighted material on the Internet it would mean that the land of sender should be lex causae, probably relating the sender by habitual residence or similar to the relevant jurisdiction. However it might be troublesome operating with such a principle on the Internet. This is because the material is often communicated in chains, e.g. in the form that the provider communicates material to the end user, which communicates it onwards to third parties. In this case, it might be questioned whether the end user is to be qualified as sender for the link in the chain originating at his site, or if the end user must be seen as a more passive station, like the cable network operator retransmitting a television broadcast originating outside the territory? Or if the end user follows a hyper link from a provider to a referred provider, and has the referred material downloaded, - is then the provider himself or the referred provider to be qualified as the sender? Several more problems are also likely to arise, for example due to the use of "mirrors" on the Internet.

Furthermore it is unlikely that all countries will accept on applying the principle of "country of origin" on the Internet. This because it for many countries in reality will mean the weakening of the protection offered to copyrighted material. If a German makes English official documents available on a German server, this has the potential of causing the same amount of damage to the English authorities as if the situation were that the German published a book in England containing the official documents. For the English authorities it may seem inconsistent that the former case is not considered an infringement, while the latter is. We do not feel sure that English authorities would have obeyed the principle of "country of origin" in a case like this. Probably the copyright legislation within the EC-countries must be harmonised to a greater extent than the situation today is, before the member states will reach a consensus in applying the principle also on the Internet. This is also the conclusion in the Green Paper of the EC Commission – *Copyright and Related Rights in the Information Society*[111].

---

[110] *Convergence* can be briefly explained as the possibilities we experience today towards that almost every types of information may be represented in digital form, and furthermore that almost all sorts of infrastructure can be utilised to carry all sorts of information. An example is that TV-cables may be used for transmitting Internet services.

[111] Brussels 19.07.1995 COM(95) 382 final

4.6.4 Law applicable for determining liability

This report will not discuss criminal liability.

The question of *qualification* might be of importance for the determination of which country's law that are to be applied on the liability question. Some intellectual property legislation, have incorporated special liability clauses, while others have not. If special liability clauses are incorporated, it must be determined whether such clauses are to be qualified as part of intellectual property law, or whether they are part of the law on civil liability. In the former case, the liability assessment will be based upon the same country's law that governs the question of whether an infringement has taken place. However, in the latter case, one is confronted with a new choice of law – deciding the *lex causae* for the liability. This is one of the traditional issues of the conflicts of laws, and the rules governing the choice of law are traditionally related to some geographical relation, for instance the *lex locus delicti.* As the discussion of jurisdiction have illustrated[112], such rules become somewhat ambiguous in our context. If the provider offers material that represent an infringement both in the country of the provider and the country of the end user, in which country did the harmful event occur? It may be argued that this was in both of the places. Certainly the examples may be made more complex.

In the latest years, one has seen a tendency towards applying the *principle of the closest connection* for determining liability questions. This will mean the application in the country to which the injury has its closest connection. Applying this principle on disputes arising on the Internet, also have its disadvantages, due to the fact that it will be difficult to in advance be certain of which law the courts will apply.

It certainly would be the best solution in our case to apply the law of damages of the same country which law governs the intellectual property issue. If different countries laws were to be applied respectively on the infringement and the liability question, one easily could end up with a situation where the action was considered a copyright infringement in country A, but not in country B, but nevertheless the law of damages in country B was to be applied.

It may be argued at least in two different ways for reaching this result: First, one may qualify the liability provisions associated to the intellectual property legislation as part of intellectual property law, and consequently they will be chosen by the same rules that governs conflict of law for issues of intellectual property. Second, one may argue that the "injury" has the closest connection to the country which law governs the intellectual property issue.

However, it is unclear how the courts are going to deal with the problem in future cases, and one should therefore take the necessary precautions to avoid being convicted.

[112] See chapter 3

5. CONCLUSION

Concluding with respect to issues where the uncertainties are as great as in private international law, can only be speculations. Trying to give clear answers might lead to further problems. Even so, we will try to give a short summary of this report as a sort of conclusion.

Considering the *jurisdiction* in Europe, the Lugano and Brussels Conventions will solve the problems of jurisdiction for private and commercial matters. For the parties addressing a court, these conventions give security as to always finding a jurisdiction. As for where this jurisdiction will be, there might be problems. And if it does, the European Court of Justice may be able to give a prejudicial judgement. Further problems arise in the field outside private law. In such cases, like advertising, public law causes problems in the digital world, mainly because they imply national jurisdiction.

As for the *choice of law*, there are different solutions for different issues. Unfortunately there are not too many international regulations available.

The choice of law in data protection, is easy to solve for a simple case, but as quickly more controllers enter the stage, the problems abound.

For contracts, and in mainly business-to-business relationships, the main rule of the 1980 Rome Convention is the party autonomy, giving them right to choose the law applicable. On the other hand problems might arise concerning the making of the contract on the Internet An other problem might be if the parties have not made a choice of law and the method of the closest connection, in the 1980 Rome Convention art. 4 is applied. Such a situation might bring great incertitude to the parties.

The applicable law which will be applied in cases where the customer is a consumer are normally the law of the country where the consumer has his habitual residence.

For advertising, one should have in mind that the law applicable is likely to be the one of the country in which the advertisement may be accessed from.

Concerning liability for loss suffered due to misleading information, the traditional rule of *lex loci delicti* must be said to compete with the method of the closest connection. This is how far we can dare to suggest a solution.

The law which are to be applied in cases concerning copyright issues, are normally the law of the country where the infringing act was carried out. However, it is not always that simple to determine this location when it comes to infringing acts that have been carried out on the Internet.

Finally this leads us to conclude that the digital world can not be said to be completely compatible with analogue world. The traditional solutions given in the existing Directives or conventions, like the Brussels Convention, are not always that suited for being applied on the digital world. The first cases dealing with these questions will therefore be very decisive. The EU may have to adopt new regulations directly applicable to the digital world. The latter solution would be welcome, implying a harmonisation of private international law in this field and offer increased predictability for the parties.

ANNEX 8 : Assistance to COSMOS : Review of the requirements report

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

ELIP
Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

COSMOS Assistance- Review of the requirement report

Intellectual Property Rights and Taxation Issues : ITM – Imke Bubert

Data Protection Issues : CRID – Sophie Louveaux

Consumer Protection issues : CRID – Anne Salaun

International Private Law : NRCCL – Morten Foss and Peter Lenda

1 Introduction

This first assistance paper from ECLIP aims at considering the legal aspects raised by the COSMOS project on the basis of the COSMOS Requirements REport, which represents the first task of assistance to be carried out for the project, as agreed with ECLIP.

This paper raises legal issues to be considered by COSMOS partners. We have particularly considered those legal issues that are specific to e-commerce scenario.

On that basis, further assistance could be agreed upon with COSMOS partners. In some parts of this paper (for instance in taxation and copyright issues), the consideration of legal issues is limited to an overall overview and should be completed with a further analysis if requested by COSMOS.

2 Intellectual Property Issues

2.1 Relevance of Intellectual Property issues in the COSMOS concept

COSMOS wants to develop a software tool to facilitate and support electronic contracting. This general tool to support contract negotiation and the conclusion of a contract by offering a brokerage service, a notary service etc. does not raise fundamental questions in the domain of intellectual property and related rights. This changes when the contracting service is applied to an economic sector which deals with the trade and exploitation of copyrighted material. The COSMOS project intends e.g. a trial application in the music business as the COSMOS partner IMP is a music publisher. In this application phase it has to be assured that license agreements are correctly concluded, but they do not differ substantially from those concluded off-line.

Copyright issues would become of greater importance if COSMOS was further involved in the execution phase of the contract and, more precisely, if on-line exploitation of copyrighted works was planned. At this stage of the project the execution phase of the contract seems to be of minor importance although a support also in this phase of the contractual relationship is not expressively excluded.

One of the questions which the project should consider is the question whether the COSMOS software tool or parts of the tool, e.g. the database established by the Brokerage Service[1], or other texts included benefit from copyright protection.

2.2 Copyright Issues in the Case Study

The Case Study chosen by COSMOS in the Requirement Analysis[2] deals with the contractual interrelationship between authors, publishers, editors, end consumer in the field of a Journal Publication. The section does not refer to copyright questions, while in practice this scenario would raise legal questions e.g. as to licensing agreements, the case study here is only given to illustrate the usage of the contracting service. The project does not foresee to edit a ready-to-use version for this economic sector. Interested parties would have to adapt the tool to the specific demands of this sector. COSMOS relies on the private companies to solve the IP related questions in their sector on their own before implementing the tool.

Therefore, the legal perspective can be neglected in the case study, as it is only meant to explain an economic scenario.

2.3 Copyright Issues in the Sector Analysis

The Sector Analysis[3] refers to a second economic field to which the COSMOS tool might be applied: the music industry. The section focuses on the perspective of a Music Publisher. Here again the question of licensing agreements which would need to be concluded using the COSMOS contracting platform is decisive, as it is also stated under 2.1.2.1 of the requirement analysis and in the specific section on Copyrights, 2.1.2.6.

The specific section dealing with copyright issues which might evolve is very short and neglects a few important points which should be mentioned.

In paragraph two of section 2.1.2.6 it is said that the "right to exploit the copyrights given to the publisher by the author is formally not touched by the way of reproduction". It is not quite clear what the author wants to indicate with this sentence and might be rather misleading. As long as only the contracts including license agreements are concluded on-line, using the COSMOS platform, this will not change the exploitation rights the music publisher needs to receive from the author in order to grant them e.g. to the record company. If, however, any kind of on-line exploitation is foreseen, e.g. providing samples of music on-line, installing a

[1] See Section 6.3.6.3 of the COSMOS D1 Requirement analysis.

[2] Section 1.9

[3] Section 2 of D1 Requirement Analysis.

music on-demand service, the music publisher needs to make sure that he also received the rights to exploit the works in this way. If he only holds the reproduction and distribution right, this will not be sufficient. For on-line services he will also need a right of communication to the public.[4] Also a music publisher who wants to use material on-line which is subject of an old license agreement, has to make sure that the new way of use is covered by this license agreement. In several European countries (Belgium, Germany and France) this has to be denied, if the means of utilisation was unknown at the time the rights were licensed. If on-line execution is planned these and further questions would have to be further examined.

In paragraph three of section 2.1.2.6 it is said that the music publisher may want to use the internet to distribute the works himself. Here it should also be stated that the music publisher has to ensure that the relevant rights were transmitted to him from the author for such an on-line use (see above).

In the same paragraph digital watermarking is mentioned as a means to protect copyrighted material used in an electronic form. In the discussion of technical solutions to the protection of copyrighted material digital watermarking is only one aspect. Electronic Copyright Management Systems (ECMS) are being developed which can be based on digital watermarks but also on cryptographic means. MCPS, PRS and Liquid Audio are e.g. have implemented a trial application of an integrated music licensing system supported by an ECMS in the frame of the European project IMPRIMATUR.[5] If the COSMOS tool shall be applied in the music business and if besides the mere contracting also on-line exploitation of works is planned, the integration of an ECMS will be necessary and probably crucial for the success of the COSMOS tool in this business sector.

2.4 Copyright Issues in the Business Model Analysis

In section 4 of the requirement analysis the new business models have not been transmitted to ECLIP, so concrete copyright issues related to these new business models can not be identified. In the constraints section 3.4, however, legal constraints are mentioned. Instead of identifying actual legal problems, the text provides for mainly a set of legal definitions related to contracts, payments etc, only considering the Italian legislation. At the very end of the Legal Constraints section, 3.4.2, legislative efforts of the Italian government are described to ameliorate the protection of copyrights. It is not clear why the section is only based on the Italian situation. The paragraph on Copyright shows that some of the relevant European Directives and International Conventions relevant to the protection of intellectual property have been identified by COSMOS. However, only two of the European directives aiming at a harmoni-

[4] See Art. 3 of the Proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, 10.12.1997, COM(97) 628, p. 56.

[5] http://www.imprimatur.alcs.co.uk/; http://www.musictrial.com/

zation of different aspects of intellectual property are mentioned, the Council directive on the legal protection of computer programs, 91/250/EEC from 14 May 1991, and the Council directive on rental right and lending right and on certain rights related to copyright in the field of intellectual property, 92/100/EEC, from 19 November 1992. Further directives relevant to intellectual property issues are the Council directive on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities 89/552/EEC[6] from 3 October 1989, the Council directive on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission, 93/83/EEC from 27 September 1993, the Council directive harmonizing the term of protection of copyright and certain related rights, 93/98/EEC, from 29 October 1993, and the Directive of the European Parliament and of the Council on the legal protection of databases, 96/9/EC from 11th March 1996. Especially the two latter directives will be significant for the software tool developed by COSMOS. Finally, COSMOS also needs to pay especially attention to the latest Proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, COM(97) 628, p. 56 from 10 December 1997. This proposal for a directive defining e.g. the frame for the right of communication to the public related to on-line service will have an enormous impact on the legal frame that the COSMOS tool needs to respect, if the project is enlarged to the execution phase.

3 Taxation Issues

3.1 Relevance of taxation issues in the COSMOS concept

Taxation issues will be of minor importance in the COSMOS project. The requirement report only refers to taxation in section 2.1.2.7 saying that the project wants to follow the development in tax law thoroughly. To give a short overview of taxation issues in electronic commerce to COSMOS a brief summary of general tax related questions is attached to this document. Concrete assistance by ECLIP in the field of taxation apart from providing general information would be recommendable, if COSMOS decides to integrate an electronic billing service into the contracting service, which seems not to be intended at this time.

[6] JO, No. L 298 , p. 23

4 Consumer Protection

4.1 Comments on the requirements report

The legislation referred to, namely the 'Act on the right to cancel front door transactions' and the 'Consumer Credit Act' is not relevant. If the first text referred to is the European Directive on *sales away from business premises*, it is not relevant since it does not apply to electronic contracts through the Internet. Provisions regarding consumer credit are more generally foreseen in the draft Directive on distance financial services.

Consequently, the remarks that follow are not relevant as more specific legislation should be examined.

Proposal:

Since contracts with consumers are foreseen in the project, consumer protection requirements will have to be complied with. As the contract concluded between a consumer and a seller in the frame of electronic commerce is a distance contract, the main European regulation applying is the Directive on the protection of consumers with respect to distance contracts (Directive 97/7/EC of 20 May 1997). The Directive is not specifically devoted to electronic commerce since its scope is general, but the rules apply to all type of contracts concluded at a distance.

For the purpose of the directive, a *consumer* is defined as "any natural person who is acting for purposes which are outside his trade, business or profession". The *supplier* is heard as "any natural or legal person who, in contracts covered by the Directive, is acting in his commercial or professional capacity".

According to the directive, the following obligations fall under the responsibility of the supplier:

1) Obligation to provide the consumer with prior information (article 4)

This obligation should be complied with 'in good time prior to the conclusion of any distance contract'. It should include:

(a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address;

(b) the main characteristics of the goods or services;

(c) the price of the goods or services including all taxes;

(d) delivery costs, where appropriate;

(e) the arrangements for payment, delivery or performance;

(f) the existence of a right of withdrawal, except in the cases referred to in Article 6 (3);

(g) the cost of using the means of distance communication, where it is calculated other than at the basic rate;

(h) the period for which the offer or the price remains valid;

(i) where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

This information shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions.

2) Obligation to provide a confirmation of information (article 5)

The consumer must receive confirmation, either in a written form or in another durable medium available and accessible to him, of the information granted prior to the conclusion of the contract. The notion of *durable medium* applies fully to electronic contracts as it allows a confirmation through e-mail, floppy disk, CD-ROM, etc.

This confirmation should be granted in good time during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him.

In addition to the prior information, the following information must be provided:

- written information on the conditions and procedures for exercising the right of withdrawal,

- the geographical address of the place of business of the supplier to which the consumer may address any complaints,

- information on after-sales services and guarantees which exist,

- the conclusion for cancelling the contract, where it is of unspecified duration or a duration exceeding one year.

One exception is foreseen by the directive for those services which are performed through the use of a means of distance communication, where they are supplied on only one occasion and are invoiced by the operator of the means of distance communication.

3) Obligation to provide the consumer with a right of withdrawal (article 6)

The supplier must give the consumer the possibility to withdraw from the contract during a period of at least 7 working days. This right of withdrawal must be opened to the consumer without penalty (the only charge that might be asked to the consumer is the direct cost of returning the goods) and without giving any reason.

The period of 7 working days begins:

- for goods, from the day of receipt by the consumer,

- for services, from the day of conclusion of the contract, or from the day on which the obligation of confirmation has been fulfilled if they are fulfilled after conclusion of the contract, provided that this period does not exceed the three-month period.

A three-month period is foreseen by the directive in case the supplier has not fulfilled his obligation of confirmation: here, the three-month period starts in the case of goods, from the day of receipt by the consumer, and in the case of services, from the day of conclusion of the contract. If the confirmation of information is supplied within this three-month period, the seven working day period shall begin as from that moment.

As a consequence to the withdrawal of the consumer, the supplier has the duty to reimburse the sums paid by the consumer as soon as possible and in any case within 30 days.

It is important to note that exceptions to this right of withdrawal are foreseen (unless the parties have agreed otherwise):

- for the provision of services if performance has begun, with the consumer's agreement, before the end of the seven working day period,

- for the supply of goods or services the price of which is dependent on fluctuations in the financial market which cannot be controlled by the supplier,

- for the supply of goods made to the consumer's specifications or clearly personalised or which, by reason of their nature, cannot be returned or are liable to deteriorate or expire rapidly,

- for the supply of audio or video recordings or computer software which were unsealed by the consumer,

- for the supply of newspapers, periodicals and magazines,

- for gaming and lottery services.

4) Obligation to perform the contract within a specific period (article 7)

Unless the parties have agreed otherwise, the supplier must execute the order within a maximum of 30 days from the day following that on which the consumer forwarded his order to the supplier. If the supplier fails to perform his side of the contract on the grounds that the goods or services ordered are unavailable, the consumer must be informed of this situation and must be able to obtain a refund of any sums he has paid as soon as possible and in any case within 30 days.
The directive leaves to the Member States the possibility to decide whether a supplier is entitled to provide a good or a service of equivalent quality and price. If this so decided, the following conditions must be fulfilled:

- this possibility was provided for prior to the conclusion of the contract or in the contract

- the consumer shall be informed of this possibility in a clear and comprehensible manner,

- the cost of returning the goods following exercise of the right of withdrawal are, in this case, borne by the supplier, and the consumer is informed of this.

5 Data protection

5.1 Review of the requirements report

The EU "guidance 95/46/EG" which is mentioned is in fact the EU **Directive** 95/46/EC.

The Directive does not need to be **"transformed"** by the member states, but needs to be "transposed" into the legislation of the member states.

One should maybe briefly mention some of the principles laid down in this directive to be data, prohibition of processing of sensitive data, data quality) along with the duties of the controller (security, notification and liability) and the rights of the data subject (right to be informed, right of access, right of rectification and right to object).

The national data protection legislation referred to in the document is the "Act on the Protection of Personal data Used in Teleservices" which can be found in the Federal Act Establishing General Conditions for Information and Communications Services of August 1st 1997.

As for its content, it does not obligate the service provider to let users choose a pseudonym or act anonymously, but states at §4(1) that the provider must offer the user anonymous use and payment under a pseudonym to the extent feasible and reasonable. This is somewhat less stringent.

Do not understand what is meant by " when it comes the payment is not due at the same time as the other party's performance is".

Furthermore the German Act imposes other provisions which could be mentioned such as the setting up of user profiles are only permissible under the condition that pseudonyms are used (§4 (4)) or the fact that personal data may be collected, processed and used by providers for the performing of teleservices only if permitted by the Act itself or some other regulation or if the user has given his consent. Similarly the provider may use the data collected for the performing of teleservices for other purposes only if permitted by the act itself or by some other regulation or if the user has given his consent. All of this is worth mentioning.

6 International Private Law

6.1 Introduction

The cosmos project is aimed to develop a support platform for business transactions across the Internet based on a generic contracting service. The businesses in question will mostly be small and medium enterprises (SMEs) with small organisations, that will benefit from electronic commerce because they will have the same means of promotion on the Internet like large multinational companies. The contracting process, though, will imply needs of assistance. The COSMOS project's goal is therefore to build an Internet-based contracting service which enables its users to negotiate, sign and settle electronic contracts without having to leave a uniform and flexible system environment.

The E-CLIP project is to assist COSMOS on some legal aspects, and the NRCCL is responsible for discussing (rather briefly) some implications of private international law. These implications are set out from the COSMOS – Requirement Analysis report of 16.09.98.

6.2 Issues of private international law to be addressed

Since the contracts, which are going to be negotiated on the Internet, may be of an international character, issues of private international law will have to be discussed. It is rather obvious that a contracting service, like the one expected from COSMOS, could relate to all kinds of legal matters. As our contribution to the COSMOS project is only meant to be rather brief, we will not have the time to address all issues of private international law. Consequently, this report will concentrate upon two or three central issues of private international law.

Contract obligations. The most important questions that need to be explored from a private international law point of view, lies within the field of contract law. The main problem is identifying the law applicable (*lex causae*) to the contract in question. Here, the 1980 Rome Convention on the law applicable to contractual obligations will be of great significance. Firstly, one will have to identify the law applicable to determine the existence of a legally binding contract. Secondly, one will have to determine which rules that are going to govern the contractual relationship. Finally, one will have to analyse whether there exist mandatory rules or similar which may limit the use of the law applied.

Within the field of contract law, one will also have to develop a discussion concerning which law that governs the question of what the effects of the use of digital signatures shall have.

Consumer protection. While the previous questions mainly address business-to-business problems, the contracting will also imply the discussion on consumer protection. The EC has in recent years been more and more concerned with the issues of consumer protection, and consequently, issued several Directives addressing these issues. In a contractual situation a business-to-consumer relation will address issues concerning mandatory rules. In a context of private international law, there are therefore several points that have to be discussed. This report will try to identify them.

Data protection. This would imply identifying the law applicable (*lex causae*) to the data processing taking place on the basis of the contractual agreements. It is presumed that the processing of personal data often will take place at the sites of both (or more) parties to the contract. The data in question may be communicated from another country through the Internet. Data mining may be included in this perspective.

This report will only offer a general discussion on the choice of law, disregarding the aspects of public law. The main issue will be the EC-Directive on data protection, and its applicability.

Finally, if time allows it, this report will seek to straight out some interlegal issues concerning the protection of intellectual propriety, and liability for misleading information.

6.3 Delimitation of a further involvement of ECLIP in International Private Law Issues

This report concentrates upon matters of *private* law. As far as possible, matters of public law, like tax law etc., will be left out of the analysis.

Furthermore, we will presume that the contracting are taking place between European parties only. Consequently, it is a study of the private international law within Europe that will be developed. The rules of private international law outside Europe will not be addressed.

ANNEX 9 : Assistance to INTERNET MEGASTORE : Legal Issues

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)

Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

Legal Issues of the Internet Megastore Project

E-CLIP

Authors : ITM (Völker Kabisch- Jan Kaestner), CRID (Anne Salaun – Sophie Louveaux), QMW (Laura Edgar), UIB (Antonia Paniza Fullana)

CONTENT

Introduction

This first assistance paper from ECLIP aims at considering the legal aspects raised by the INTERNET MEGASTORE project, which represents the first task of assistance to be carried out for INTERNET MEGASTORE project, as agreed with ECLIP.

This paper raises legal issues to be considered by INTERNET MEGASTORE partners. We have particularly considered those legal issues that are specific to e-commerce scenario.

On that basis, further assistance could be agreed upon with INTERNET MEGASTORE partners. In some parts of this paper (for instance in taxation and copyright issues), the consideration of legal issues is limited to an overall overview and should be completed with a further analysis if requested by Internet Megastore.

1 Taxation Issues[1]

Two taxation issues appear of interest with regard to Internet Megastore. They concern value added tax (VAT) and tax administration and compliance.

1.1 Value added tax

According to the slides presented on the meeting, Internet Megastore is not involved in the delivery of the goods, neither between supplier (or the wholesaler) and the retailer nor between the retailer and the customer. It just provides a structure to handle the necessary marketing activities. As far as I understand from the slides, this service is supplied to the retailers. Only the tax treatment of such services needs to be addressed. Perhaps the possibility of issuing an electronic invoice might also be of interest.

1.2 Tax administration and compliance

Addressing electronic commerce transactions national tax authorities start to focus on intermediaries to collect taxes or at least to gather information. However, since the conventional

[1] Author : Volker Käbsich - ITM

delivery chains remain intact in the presented scenario Internet Megastore should not be affected by such measures. Nonetheless, the development in this field must be watched.

1.3 Summary

As only minor taxation issues need to be addressed, four man-days should be sufficient to perform the assistance. It might be necessary to extend this amount if more (taxable) services are provided between the participants.

2 Copyright Issues[2]

The note of the meeting on the Internet Megastore Project as of October 5th, 1998, does not mention a need in assistance on copyright. However, we think it necessary to point out that there are some problems with regard to copyright which might arise out of the projects activity.

2.1 Presentation of product information

As far as we understand the project, Internet Megastore seeks to establish a virtual mall as a platform upon which retailers and/or wholesalers may present themselves and get into contact with the end user (consumer).

The common method to sell goods via the Internet through virtual malls is by presenting the goods in picture and with product information (maybe even in form of a multimedia catalogue) on a website. This involves heavy activity in the field of copyright which will have to be considered (and which is partly known from the publication of product catalogues in the off-line world). Especially in a situation where a retailer provides Internet Megastore with information this may result in problems of copyright:

- Internet Megastore will have to make sure that the product information they publish on the Internet is either not a copyrighted work or licensed. Here, it is important for the project to know which parts of the multimedia catalogue are protected by copyrights or neighbouring rights, who the rightholders are and which exploitation right is needed (reproduction and public performance).

- The acquisition of licenses might be difficult in case a retailer provides the information. Here, Internet Megastore will have to make sure that the retailer is the rightholder and en-

[2] Author : Jan Kaesyner - ITM

titled to license the work to Internet Megastore. Otherwise, Internet Megastore will have to acquire a license directly from the author.

- Furthermore, with the establishment of a website, Internet Megastore may need to protect the works they publish in order to promote sales against copyright infringement. This is yet difficult and should be considered during the licensing negotiations.

As Internet Megastore will not benefit from a statutory licence, the project might need assistance for drafting the necessary licensing agreements. This assistance could be carried out by proof-reading pre-existing contracts or by drafting the respective provisions.

2.2 Protection of the Internet Megastore website

In case the website will use sources other than those on the Internet Megastore server there may be some copyright problems as well the project should be aware of (hyperlinking, framing). The project might be interested in getting to know which parts of the Internet Megastore website are protected by copyrights or neighbouring rights and who the rightholders are. Furthermore, the project may want to know by which acts their copyrights are infringed and how to can protect themselves against such infringement.

2.3 On-line delivery and trademark issues

From the note of the meeting it is not clear whether Internet Megastore envisions on-line delivery of copyrighted works. The project so far seems to concentrates on groceries and furniture but if the project includes retailers in the fields of books, videos, audio material or the like, many difficult copyright questions may arise.

It is unlikely that Internet Megastore will be interested in trademark law-related assistance. Questions would only arise if the project used a third parties name as domain.

2.4 Summary

To work out the "catalogue" and website problems we estimate the need of four man-days (two for working out the licensing issues, two for the copyright problems with regard to a website). In case that Internet Megastore wants ECLIP to analyse specific pictures, texts, video clips or other material used in the website, the number of man-days has to be augmented.

3. Electronic Payment Issues[3]

3.1. Framework of the Internet Megastore technology

In order to understand the legal issues relating to payment systems it is necessary to determine exactly how the payment methods are to be structured.

Either the payment can be made directly to the retailer by cheque, cash or bank transfer or by electronic means by credit card or smart card.

When payment takes place electronically who receives the payment? Is one payment made to the virtual mall operator for goods bought in all of the shops or is payment made to each retailer separately?

If payment is made to the virtual mall operator then payment must be distributed to the individual retailers. It would appear that the mall operator acts as a payment intermediary by collecting the payments information on the host web server then transmitting it to the payment processor server before the details are sent to the merchant bank

At what stage does payment take place? Is it after the retailer has confirmed the customer's order? Does the retailer then inform the customer to pay? Is it ever the case that the customer will pay and then the retailer will be unable to fulfil the order request?

3.2. Potential Legal Issues

If it is the case that the virtual mall operator acts as an intermediary by facilitating payment then this may give rise to certain responsibilities on the part of the virtual mall operator.

a) Contractual Issues

The contractual relationships between the mall operator and retailer and between the mall operator and the payment system will have to be carefully considered. Points to be considered include:

Who is responsible for refunding the customer if payment has been made and the retailer is unable to supply the goods?

[3] Author : Laura Edgar - QMW

Who will bear the risk if credit cards are not verified immediately online?

b) Security issues

What security methods are foreseen for protecting credit card details?
SSL, SET?
Who is liable for security breaches in the payment system?

This would be determined by the contractual relationship between the payment system and the virtual mall operator if he is providing the payments structure or between the retailer and the payment system.

c) Data protection

It will be important to examine the use made by the mall operator of the payments information. In particular whether it is intended to use the information collected for reasons other than simply facilitating payment such as marketing purposes. In this case the mall operator may come into conflict with the principles of the EU Data Protection Directive as implemented in national law. Another potential conflict will arise in relation to the transfer of personal data to countries outwith the European Union which do not have adequate levels of data protection. This would arise where use is made of a non-European payment systems operator and the mall operator transmits personal data to them.

4. DATA PROTECTION[4]

4.1. Introduction

The first question one has to ask oneself when looking at the Internet Megastore project is whether data protection law applies and if so which national law will apply?

According to the EU directive 95/46/EC, with which national data protection laws must comply, the applicable law is that of the country in which the controller is established (by "establishment" §19 of the directives' recitals means "the effective and real exercise of an activity through stable arrangements"). In order to determine the data protection principles to

[4] Author : Sophie Louveaux - CRID

be respected, one must therefore answer two questions: firstly, is personal data being processed and secondly who is the "controller" of the processing?

4.2. Personal data

Article 2 of the EU directive defines personal data as "any information relating to an identified or identifiable natural person; an indentifiable person is one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

The directive does not therefore include in its scope data relating to legal persons. However the Italian Data Protection Act (Law n° 675 of the 31.12.1996) does provide for the protection of data relating to legal persons and any other body or association (see article 1.1 of the Act).

The Internet Megastore project involves the processing[5] of data relating to clients and data relating to retailers and wholesalers.

As for data relating to clients two types of data can be identified:

- Data collected directly from the data subject when purchasing goods/services. This data is that necessary for the purchase and delivery of the goods or services and the necessary data for the payment (if the payment is made by bank transfer or credit card).

- Consumer information collected through the use of the network in order to establish consumer profiles.

As for data relating to retailers and wholesalers, it is not exactly clear from the present description of the service, what type of data is collected and processed. What is clear however is that if the Italian data protection law should apply (this will depend on whom can be qualified as controller, see below), the processing of such data will be covered by the law and must respect the data protection principles.

[5] By processing the directive means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage,..."

4.3. Controller

It is important to determine who is the controller of the data not only because the establishment of such a controller determines the national law applicable (see above) but also because the controller is the primary responsible for respecting the data protection principles laid down in the directive and complying national legislation.

The controller is defined by the EU directive as "the natural or legal person, public authority, agency or any other body which alone or jointly with other determines the purposes and means of the processing of personal data.

From the available description of the Internet Megastore project, one could assume that both the retailer and Internet Megastore could be considered as controllers with respect to the processing of different type of data.

The retailer can be considered as the controller with respect to the processing of consumer data necessary for the sale and delivery of goods and services. Indeed the retailer is processing data for a purpose and with means defined by him. (Therefore, if CFP, the Italian consortium of companies is a retailer processing consumer data, the Italian legislation will apply).

Internet Megastore can be considered as the controller with regard to the processing of consumer data for consumer monitoring and of retailer and wholesaler data.

Now that it has been established that personal data is being processed, and by whom, one must identify the data protection principles to be complied with if one wishes to respect the EU directive.

4.4. Data protection principles

According to article 6 of the directive, personal data must be processed fairly and lawfully. Fair processing implies a maximum of openness. Lawfulness implies that the data protection principles must be respected. The data must be processed for legitimate, specified and explicit purpose and must not be further processed in a way incompatible with that for which the data was initially collected. This implies that the controller must determine at the outcome what the data is being collected for (purchase and delivery of goods...), must inform the data subject of this purpose (see later right to be informed), and must not process the data for any purpose which is not in line with the purpose for which the data was initially collected without informing the data subject. The processing of data for statistical purposes is not, according to

the directive, considered as incompatible providing the Member states provide the adequate safeguards. The consumer profiling by the actual retailer who initially collected the data may therefore not always be considered as incompatible.

Article 7 lays down grounds on which the data processing must be based. In the context of the Internet megastore applications, the processing could either be based on the data subject having given his unambiguous consent or if the processing is necessary for the performance of a contract to which the data subject is a party or in order to take the steps at the request of the data subject prior to the entering of the contract.

As for data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life», it is in principles prohibited unless it can be based on grounds laid down in article 8.2. of the directive. Personal profiling based on such data must therefore in principle be prohibited.

Data quality implies that the data must be adequate, relevant and not excessive with regard to the purpose for which it was initially collected.

The data must be accurate and kept up to date. Every reasonable step must be taken to ensure that data, which are incomplete or inaccurate, are either erased or modified.

The data must not be kept in a form which permits identification of the subjects for longer than is necessary for the purposes for which the data were collected or for which they were further processed. This implies that once the customer has completed the purchase of his goods and that he has been adequately billed for such a service, his data must not be further stored by the retailer unless necessary.

4.5. Rights of the data subject

The data subject is granted with a number of rights. It is up to the data controller to ensure that these rights are respected.

The data subject must be informed of a certain number of items. If the data is collected directly from the data subject (this is the case for example, for the retailer collecting data from the customer when ordering goods), article 10 provides that the data subject must be informed at least of the identity of the data controller and the purpose of the processing. He must be further informed of any information such as the recipients or categories of recipients, whether

replies to questions are obligatory or not, as well as the consequences of the failure to reply if such information is necessary to guarantee fair processing in respect of the data subject.

If the data is not directly collected from the data subject (as is the case for Internet Megastore who is collecting data through the retailers), the data subject must be informed either when the data is first recorded or when the data is first communicated. Information covers the same

data as that mentioned in article 10 plus the categories of data concerned if necessary to ensure fair processing.

Article 11.2 does however provide for an exemption to the duty to inform for statistical purposes if the provision of such information proves impossible or would involve a disproportionate effort. This could be the case if Internet Megastore only receives statistical data from the retailers with no direct contact with the consumers.

The data subject also has the right to have the confirmation of the existence of data about him being processed and information about the purposes of the processing, categories of data and categories of recipients. He may also receive the communication in an intelligible form of the data undergoing processing and of any available information about the sources of the data.

This right of access of the data subject to his data must be granted without constraint at reasonable intervals and without excessive delay or expense. If appropriate the data subject is granted with the right to the rectification, erasure or blocking of data in particular because the data is incomplete or inaccurate.

The data subject also has the right, on compelling and legitimate grounds, to object to the use of his data. This right is granted unconditionally as concerns data collected and used for direct marketing purposes (see article 14.b of the directive). This right to object could mean that the consumer in the Internet Megastore project object to the processing of his data for promotional purposes.

Finally, the data subject is granted with the right not to be subject to individual automated decisions that is to say decisions which produce a legal effect concerning him or which significantly affects him and which is based solely on automated processing of data intended to evaluate certain aspects relating to him such as his creditworthiness, reliability, conduct,...

4.6. Duties of the controller: Notification, security and confidentiality

The controller of the data must notify a national supervisory authority prior to the processing of the data.

The controller must also ensure that the appropriate technical and organisational measures are set up to protect personal data against accidental or unlawful destruction or loss of the data. These measures must be taken with regard to the risks represented by the processing and the nature of the data and must be taken with regard to the state of the art and the cost of their implementation. Persons processing data under the authority of the controller may only process the data if required to do so by law or under the instructions of the controller. The controller must lay down instructions to any person processing data on his behalf (processor) in a contract or legally binding act.

4.7. Transborder data flows

Personal data may only be transferred to countries outside the European Union if this state offers an adequate level of protection according to the Member states and the European Commission. The Commission has developed a series of criteria in this respect in its article 29 Working Group. Any transfer of data must therefore be to a country which affords this protection unless the transfer can be based on an exemption found in article 26 of the directive an notably if the data subject has given his consent unambiguously to the proposed transfer or if the transfer is necessary for the performance of a contract between the data subject and the controller.

5. Consumer protection issues[6]

5.1. Introduction

The virtual outlet imagined in the Internet Megastore project is, as far as consumers are concerned, linked to the distance contracts directive of 20 may 1997[7]. The sale of products or services foreseen in the virtual outlet through the use of Internet is seen as a distance contract according to article 2 of the directive: a distance contract is heard as "any contract concerning goods or services concluded between a supplier and a consumer under an organised distance sales or service-provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded".

The sales contract foreseen in the Internet Megastore project fall under this definition, which implies that all the requirements of the directive should be complied with.

5.2. Levels of relations within the project

The project implies different levels of relations:

- the first relation is illustrated by the first contact of the consumer with the platform, i.e. Internet Megastore,

- another is the relation between Internet Megastore and the seller: once a consumer has contacted the platform and ordered a good, the seller is informed about this ordering by Internet Megastore,

- a another relation is the direct contact between the consumer and the seller.

Internet Megastore cannot be considered as the co-contractor of the consumer: his job is to act as an *intermediary* between the consumer and the seller, not to act on behalf of the seller.

---

[6] Author : Anne Salaun - CRID

[7] Directive 97/7/EC of 20 May 1997 concerning the protection of consumers with respect to distance contracts O.J.E.C. L.144/19 of 4.06.1997.

Thus, the contract will be directly concluded between the consumer and the seller. No specific obligation will be imposed upon Internet Megastore with regard to the distance contract directive, as Internet Megastore is not considered as the supplier[8].

5.3. Management of promotional information

The project aims at developing its activity of remote sale through direct contacts with consumers. Consumers will therefore be individually contacted by Internet Megastore (either through their e-mail address or physical address), and commercial communications will be sent.

In this respect, it is important that Internet Megastore partners note the following principles with regard to commercial communications:

⇒ responsibility of the partner with regard to the content of the communication: the information presented in the communication bounds the advertiser;

⇒ the principle of a right for the consumer to oppose to commercial communication on the basis of article 14 (b) of the Directive on the protection of individuals with regard to the processing of personal data and the free movement of such data[9], and on the basis of article 10 § 2 of the distance contracts Directive which lays down the *opt-out* principle: "means of distance communication which allow individual communications may be used only where there is no clear objection from the consumer";

⇒ in consequence, before sending commercial communication through the private address of the consumer, the partners should first take the necessary arrangements to know if the consumer has clearly objected to receive individual communications, and inform the consumer about his right to object, free of charge, to receive individual commercial communications;

⇒ provisions regulating misleading and comparative advertising[10] at the European level should also be complied with.

---

8 See *infra* the definition of the supplier given by the directive.

9 Directive 95/46/EC of 24 October 1995 *O.J.E.C.* L.281/31 of 23.11.1995.

10 Directive 97/55/EC of the European Parliament and the Council of 6 October 1997 concerning misleading advertising so as to include comparative advertising, available on the Internet: http://www.europa.eu.int/comm/dg24/policy/developments/comp_adve/comp_adve02_en.html

5.4. Compliance with the distance contract directive

The seller, be it retailer, wholesaler or supplier, will be the one in charge of fulfilling the obligations set forth in the directive under the qualification of 'supplier'. The supplier is heard as "any natural or legal person who, in contracts covered by the Directive, is acting in his commercial or professional capacity".

For the purpose of the directive, a consumer is defined as any natural person who is acting for purposes which are outside his trade, business or profession

According to the directive, the following obligations fall under the responsibility of the supplier:

1) Obligation to provide the consumer with prior information (article 4)

This obligation should be complied with 'in good time prior to the conclusion of any distance contract'. It should include:

(a) the identity of the supplier and, in the case of contracts requiring payment in advance, his address;

(b) the main characteristics of the goods or services;

(c) the price of the goods or services including all taxes;

(d) delivery costs, where appropriate;

(e) the arrangements for payment, delivery or performance;

(f) the existence of a right of withdrawal, except in the cases referred to in Article 6 (3);

(g) the cost of using the means of distance communication, where it is calculated other than at the basic rate;

(h) the period for which the offer or the price remains valid;

(i) where appropriate, the minimum duration of the contract in the case of contracts for the supply of products or services to be performed permanently or recurrently.

This information shall be provided in a clear and comprehensible manner in any way appropriate to the means of distance communication used, with due regard, in particular, to the principles of good faith in commercial transactions.

2) Obligation to provide a confirmation of information (article 5)

The consumer must receive confirmation, either in a written form or in another durable medium available and accessible to him, of the information granted prior to the conclusion of the contract. This confirmation should be granted in good time during the performance of the contract, and at the latest at the time of delivery where goods not for delivery to third parties are concerned, unless the information has already been given to the consumer prior to conclusion of the contract in writing or on another durable medium available and accessible to him.

In addition to the prior information, the following information must be provided:

- written information on the conditions and procedures for exercising the right of withdrawal,
- the geographical address of the place of business of the supplier to which the consumer may address any complaints,
- information on after-sales services and guarantees which exist,
- the conclusion for cancelling the contract, where it is of unspecified duration or a duration exceeding one year.

One exception is foreseen by the directive for those services which are performed through the use of a means of distance communication, where they are supplied on only one occasion and are invoiced by the operator of the means of distance communication. However, this exception does not seem to be relevant for the project since no on-line performance is foreseen for the time being.

3) Obligation to provide the consumer with a right of withdrawal (article 6)

The supplier must give the consumer the possibility to withdraw from the contract during a period of at least 7 working days. This right of withdrawal must be opened to the consumer without penalty (the only charge that might be asked to the consumer is the direct cost of returning the goods) and without giving any reason.

The period of 7 working days begins:

- for goods, from the day of receipt by the consumer,

- for services, from the day of conclusion of the contract, or from the day on which the obligation of confirmation has been fulfilled if they are fulfilled after conclusion of the contract, provided that this period does not exceed the three-month period.

A three-month period is foreseen by the directive in case the supplier has not fulfilled his obligation of confirmation: here, the three-month period starts in the case of goods, from the day of receipt by the consumer, and in the case of services, from the day of conclusion of the contract. If the confirmation of information is supplied within this three-month period, the seven working day period shall begin as from that moment.

As a consequence to the withdrawal of the consumer, the supplier has the duty to reimburse the sums paid by the consumer as soon as possible and in any case within 30 days.

It is important to note that exceptions to this right of withdrawal are foreseen, unless the parties have agreed otherwise:

- for the provision of services if performance has begun, with the consumer's agreement, before the end of the seven working day period,

- for the supply of goods or services the price of which is dependent on fluctuations in the financial market which cannot be controlled by the supplier,

- for the supply of goods made to the consumer's specifications or clearly personalised or which, by reason of their nature, cannot be returned or are liable to deteriorate or expire rapidly,

- for the supply of audio or video recordings or computer software which were unsealed by the consumer,

- for the supply of newspapers, periodicals and magazines,

- for gaming and lottery services.

4) Obligation to perform the contract within a specific period (article 7)

Unless the parties have agreed otherwise, the supplier must execute the order within a maximum of 30 days from the day following that on which the consumer forwarded his order to the supplier. If the supplier fails to perform his side of the contract on the grounds that the goods or services ordered are unavailable, the consumer must be informed of this situation and must be able to obtain a refund of any sums he has paid as soon as possible and in any case within 30 days.

The directive leaves to the Member States the possibility to decide whether a supplier is entitled to provide a good or a service of equivalent quality and price. If this so decided, the following conditions must be fulfilled:

- this possibility was provided for prior to the conclusion of the contract or in the contract

- the consumer shall be informed of this possibility in a clear and comprehensible manner,

- the cost of returning the goods following exercise of the right of withdrawal are, in this case, borne by the supplier, and the consumer is informed of this.

The project should therefore pay attention to the national legislation implementing the directive with regard to an equivalent product or service, and to the rules set forth.

5.5. Gathering of consumer information to adapt product offering

Data collecting on the consumer in order to adapt the offer should pay attention to privacy issues (*see* for this particular point the assistance provided with regard to privacy issues).

6. CONTRACT LAW[11]

6.1. Introduction

As different national laws of contracts are involved, I will only extract the common legal issues.

We are in front of a "virtual commercial center" in which different shops use a space in the mall, where they offer their goods and services.

There is a triangular system, with three parts acting in it: the **mall**, the **shops** and the **consumer**, in a double structure:

- Contracts between the mall and the shops. It is performed off line.

- The web and the way it works (on line).

6.2. Conclusion of the contract.

A.- Invitation to offer, offer and acceptance.

It is very important to achieve a clear meaning for the visitors interaction.

The content of the messages and the surrounding web pages will serve to interpret when the visitor has sent a contractual acceptance, a contractual offer or a mere invitation to offer.

[11] Author : Antonia Paniza Fullana - UIB

The use of digital signatures is generally not useful to resolve this, as they have not a sole meaning.

B.- The unity of the web contracting and general terms included.

The messages sent by clicking and writing on a commercial web page will not be considered as beeing independent of the total presentation of the web page from where they are sent.

The whole web pages and messages compose an indissoluble unity. From this principle comes the next subject about the general terms laws.

Contractual rules included in web pages should be considered as general terms and therefore should be in accordance with specific laws about general terms.

The law about this subject is the Directive 93/13/EEC, on unfair terms in consumer contracts, adding to this, all laws that each member of the EU has own country.

The 5 of April Directive, n. 93/13, includes the regulation on contracts relatives to goods and services in which takes part consumers and enterprises. It is very important for the consumer protection. Also this Directive establishes a system that allow judicial appreciation (evaluate evidence) on contracts including abusive clauses.

> COUNCIL DIRECTIVE 93/13/EEC, UNFAIR TERMS IN CONSUMER CONTRACTS.
>
> - Article 1.1: "The purpose of this Directive is to approximate the laws, regulation and administratives provisions of the Member States relating to unfair tems in contracts concluded between a seller or supplier and a consumer".
>
> - Article 3: 1. "A contractual term which has not been individually negotiated shall be regarded as unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties´ rights and obligations arising under the contract, to the detriment of the consumer.

2.- A term shall always be regarded as not individually negotiated where it has been drafted in advance and the consumer has therefore not been able to influence the substance of the term, particularly in the context of a pre-formulated standard contract.

The fact that certain aspects of a term or one specific term have been individually negotiated shall not exclude the application of this Article to the rest of a contract if an overall assessment of the contract indicates that it is nevertheless a pre-formulated standard contract.

Where any seller or supplier claims that a standard term has been individually negotiated, the burden of proof in this respect shall be incumbed on him.

3.- The Annex shall contain an indicative and non-exhaustive list of the terms which may be regarded as unfair".

But also legal rules on the inclusion requirements of general terms should be emphasized in electronic commerce. The organisation of the web pages should make general terms clearly avalaible to the web visitor. This commandament is not fulfilled if general terms are presented in a mix with lots of advertising and information links, pages and frames. It is very important in electronic commerce the web page organisations. They must be clear to the web visitor.

Pay attention to another fact: the order in which pages are hyperlinked is not necessarly the order in which they are visited.

C.- When and where the contract is performed.

Legal effects (applicable law and competent judge) relating to **where** a contract is concluded are progressively disappearing in modern law. There are, nevertheless, still some legal consequences tied to the place where a contract is formed, especially in internal national laws.

But, there are several difficulties to determinate **when** or **if** the contract is concluded.

Some theories have been developed to solve this question. Nowadays there is a majority trend towards the reception theory. According to this theory, the moment of the conclusion of the contract is when the acceptance arrives to the retailer, and he has the possibility to know the acceptance.

This trend can be intensified with a contract clause, in the relation between the shop and the consumer.

6.3. Information and Advertising.

A.- Duty to inform.

Information is one of the axis of the european programmes on the consumer protection and it is one of the main principles lying under the directives which form the european consumer law.

The duty to inform, what does really means?

- It´s a real legal duty and therefore its breach provoques legal consequences both in contract law and in tort law.

- It´s a relative duty, more than a duty to inform is a duty to get the consumer informed and therefore depends of the need of information as average consumer has. It should be taken into account that there is still a general lack of information of how Internet runs.

- It´s a large duty. It includes not only the price and main features of the products, but also other colateral items such as the legals rights of the consumer, risks,... In electronic commerce it includes the way of contracting, that is, the useful information of how the web contracting gets.

- It is an overlaped duty, I mean that a producer could not use as a defense that another party involved in the preparation or perfomance of the contract has not comply with his duty to inform.

In this case, not only the shop has the duty to inform, it seems that the mall should have some kind of information obligation, perhaps about general questions.

B.- Advertising.

Web publishing is a form of advertising, therefore, electronic commerce web pages are subjected to advertising laws.

C.- The shop is entailed by the information or advertising of the mall.

The relationship between the mall and the shops is hierarchic. Consequently, all the rules created by the mall must be observed by the shops whose web pages are hosted in the server of the mall holder.

6.4. Contract Liability

A.- Relationship between the consumer and the shop.

See the part on consumer protection

B.- Relationship between the mall and the consumers.

If there are differences between the real offer of the shop and the information offered to the consumer by the mall and they are produced by technical or organisation failures, who is entailed by the information which has been given?

C.- Contracts between the mall and the shops.

We can find two different contracts:

A.-The first one can be: a **lease (rent) contract.** The shops resides in the mall's server, so the mall rents a place to the shops.

B.- Also, there is a **service contract.** The mall filters the incoming external data into the systems catalogues, redefines the shelf management rules using the statistical data provided by the consumer monitoring... (from Internet Megastore meeting).

Contract liability arises when in any of the types of the contracts, one of the parties breaks his obligations.

6.5. Evidence and Authentication.

A.- Authentication of the shop / Digital signature.

The security is very important in the electronic commerce. The trust of the consumer in the electronic commerce depends of this security.

- AUTHENTICATION.

In the electronic commerce, the security is very important. So, the authenticity of the server is a good solution. For this, there are protocols like SSL, that provides a secure channel for communicating between web clients and web servers.

Before sending confidential data to an authenticated site, the client inspects the side server certificate to confirm the identity of the site. The server certificate is provided by a trusted Certificate Authority (C.A.).

- DIGITAL SIGNATURE.

Digital signature can be used to endorse an electronic document in a way that can be later validated for authenticity

Several different methods exist to sign documents electronically varying from very simple methods (E.G. inserting a scanned image of a hand-written signature in a word processing document) to very advanced methods (E.G. digital signatures using "public key cryptography").

Electronic signatures allow the recipient of electronic send data to verify the origin of the data (authentication of data source) and check that the data are complete and unchanged and thereby safeguard their integrity (integrity of the data).

The digital signature is an essential tool for providing security and developing trust on open networks and we must know its real meaning as a key issue for electronic commerce.

Internet is a global, but insecure, network and Cryptography can contribute greatly to the transactional security that Internet commerce lacks. Cryptography must solve four basic questions about security in electronic commerce:

- Confidentiality of the data transaction.

- Integrity: protection agains data modification.

- Authentication of the different partners and other entities involved.

- Non repudiation: no entity should be able to deny that he has sent a message.

In this case, the question is: ¿who has to autenthify, the mall or the shop?

B.-The proof of the acceptance reception.

One characteristic of digital signatures which is not usually mentioned is that they do not make the same evidence available to both parties to an electronically formed contract. As proof is not provided to the offeree demonstrating that the offeror has received the offeree´s message of acceptance, it could be said that only the offeror is in possesion of the contractual document. Only a functional acknowledgement of receipt digitally signed by the offeror provides evidence of the receipt, but if this is not produced the offeror is a stronger position. It may be concluded, therefore, that either equal position of the parties towards evidence is in-

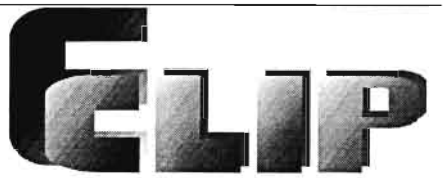
significant in an economic perspective (as it seems to be the case in EDI), or that a neutral thirth party is needed to provide evidence of the receipt of messages.

The role of such a third party should be defined and its neutrality verified, either on a contractual basis or on a legal one (and this is especially needed for consumers.

There is, nonetheless, an economic approach that may counterbalance this "evidence" approach. As regards EDI we have identified the forces that produce contractual equilibrium despite the unequal distribution of means of proof or simply the lack of means of proof. Moving on to E-Commerce we can identify consumer protection instruments as a new and characteristic source of pressure. This may range from a single letter from a consumer published in a newspaper, tests in especialised consumer "media", to sanctions imposed by consumer protection authorities. It should be noted that for consumer who do not know each other, protesting because a supplier refuses to be contractually bound, do not constitute clear evidence of a specific contract having been accepted, but do enable consumer protection authorities to impose a sanction for mal practice.

ANNEX 10 : Assistance to CYBERBRAND : Data protection issues

BUREAU VAN DIJK, MANAGEMENT CONSULTANTS (BvD)
CENTRE DE RECHERCHES INFORMATIQUE ET DROIT
FACULTES UNIVERSITAIRES NOTRE-DAME DE LA PAIX NAMUR (CRID)
CENTRO DE ESTUDIOS DE DERECHO E INFORMATICA DE LES ILLES BALEARS
UNIVERSITAT DE LES ILLES BALEARS (UIB)
GMD - FORSCHUNGSZENTRUM FÜR INFORMATIONSTECHNIK
INFORMATION TECHNOLOGY LAW UNIT OF THE CENTRE FOR COMMERCIAL LAW STUDIES
QUEEN MARY AND WESTFIELD COLLEGE (QMW)
INSTITUT FÜR INFORMATIONS-, TELEKOMMUNIKATIONS- UND MEDIENRECHT
WESTFÄLISCHE WILHELMS-UNIVERSITÄT (ITM)
NORWEGIAN RESEARCH CENTER FOR COMPUTERS AND LAW
UNIVERSITY OF OSLO (NRCCL)



Electronic Commerce Legal Issues Platform

ESPRIT Project 27028

Electronic Commerce Legal Issues Platform

CYBERBRAND – Overview of Privacy Issues

CONRAD application

Author : Sophie Louveaux (CRID)

CONTENT

1 Introduction

The European Union directive on the protection of individuals with regard to the processing of personal data[1] was expected to be transposed into the legislation of the Member States by October the 24th 1998 and from this date is a legally binding instrument. While the directive may require some modifications in the European countries' law, most of these countries already embody the principles of the directive. An overview of the regulatory framework in action in the context of electronic commerce in the European Union cannot therefore avoid the analysis of this directive[2].

In Germany, article 2 of the Federal Act Establishing the General Conditions for Information and Communication Services[3] entitled "Act on the Protection of Personal Data Used in Teleservices"[4] will apply, according to §2 of the Information and Communication Services Act to "all electronic information and communication services which are designed for the individual use of combinable data such as characters, images or sounds and are based on transmission by means of telecommunications (teleservices)" and in particular to goods and services offered and listed in electronically accessible data bases with interactive access and the possibility of direct order. A project such as CYBERBRAND may therefore fall within the scope of the TTDSG.

The aim of this paper is, therefore, to outline the main obligations arising from these legal instruments which must be respected in the CYBERBRAND project.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ No L 281, 23.11.1995, p.31 (hereinafter 'directive').

[2] We will leave out the specific issue of the transfer of personal data outside the European Union seeing as these types of transfers are not envisaged in the CYBERBRAND projects.

[3] Informations-und Kommunikationsdienste-Gestz – IuKDG of August 1 1997 (hereinafter Information and Communication Services Act) ;

[4] Teleservices Data Protection Act – Teledienstedatenschutzgestetz (hereinafter 'TDDSG')

2 Scope and Identification

2.1 Personal data

The European directive applies to the processing of personal data wholly or partly by automatic means[5]. One of the first questions that arise therefore is to determine whether or not personal data is being processed in the context of the electronic commerce activities developed by CYBERBRAND.

The Directive adopts a very broad definition of the term "personal data" so as to include any information relating to an identified or identifiable person ("data subject"). The person may be "directly" identified (by reference to his name, for example) or can be "indirectly" identified by reference to specific characteristics of that person, in particular by reference to an "identification number", or to one or more factors specific to his "physical, psychological, mental, economic, cultural or social identity". It must be underlined that the directive does not therefore apply to data regarding legal persons[6].

Two types of data can be identified in the CYBERBRAND project: data collected for the use of the service (name, first name, address, telephone number, customer-ID...) and data extracted from the use of the web site.

2.1.1 Collected Data

A distinction must be made here between existing customers entering the site and new prospective customers. In the context of existing customers even if they do not enter their actual name, but submit a customer or card number when entering the website, there is no doubt that personal data about that customer is being processed since this number is linked to identification of the customer (indirectly identifiable person in the terms of the directive).

As for new customers entering the site without necessarily purchasing any goods, they could be asked upon entering into the site to fill in a form requesting personal data and in this case the directive will apply. However if the data subject himself introduces no data, will the directive still apply?

---

[5] See article 3.1 of the directive.

[6] It must be pointed out however that some national laws have extended the scope of the directive to legal persons (see Italian Data Protection Law of 1997).

Users inevitably leave an electronic trace when entering the Net. This trace takes the form of an IP address (Internet protocol address), i.e. a series of numbers. Whether or not the IP address relates to an "identifiable" person is not straightforward.

A distinction must be made between a dynamic IP address and a fixed IP address:

A dynamic address is a numeric routing number that is allocated by the Internet Access Provider (IAP) to a computer for a specific session on the Internet. The access provider is the one who can link the IP address to an identified person or computer. Very often, however, the user is asked by the host to give his name or e-mail address. The host can then "put a name" on the IP address and follow the person during all his operations. Unless the user reveals further information or there exists a link between the host site and the IAP, the sites that are being visited can only associate the IP address with the IAP but not with the user of the Internet. The IAP rather than the site itself, therefore, can identify the user or the computer linked to the IP address.

In contrast a fixed IP address will always identify the same specific computer for every session on the Internet. However once the computer has been identified, does this mean that we are in the presence of personal data that relates to an "identified" or "identifiable" individual?
According to the recitals of the directive (see §26), "to determine whether a person is identifiable, account should be taken of all the means likely to be used either by the controller or by any other person to identify the said person". Some Member States have interpreted this to mean that the data relates to an identifiable person as long as the controller or any third party is able to identify the person. This would mean that IP addresses must be considered as personal data as long as the IAP is able to link the IP address to a particular person rather than to an aggregate of persons. Indirectly identifiable information is therefore limited to information that can be reasonably linked to an identified person. The answer to this issue will depend on the ease and probability of linking such addresses to a specific person[7].

A fixed IP address is more likely to be qualified as personal in the same way as licence plate numbers or telephone numbers have been qualified as personal data by the national data protection authorities. This is even truer in the context of the

[7] See on this subject « Privacy, Data Protection and Copyright : Their Interaction in the Context of Electronic Copyright Management Systems », Imprimatur, Institute for Information Law, Amsterdam, June 1998, p.14.

services offered by CYBERBRAND, which rely on the identification of the person so as to establish a personalised service.

2.1.2 Extracted data

Extracted data covers any data which is not directly submitted by the data subject himself but is deduced from consumer behaviour (which products are of particular interest for the consumer, which products are bought, which banners lead the consumer to the website...) or from the use of the web site, for example. To the extent that this information can be linked to an identified or identifiable individual, it must be considered as personal data.

If the consumer does not identify himself, he will not necessarily be identifiable from his consumer patterns or his visits to certain websites. Purchases may not necessarily correspond to a person's needs or profile. In some cases therefore the connection between the product and the purchaser's own habits or tastes may be too remote: a buyer could be buying for someone else, for example. The link will depend on several factors such as the nature of the product and the nature of the transaction (e.g. a one-off transaction will tend to say less about the consumer than a series of purchases involving an interest in certain themes).

Similarly one can question as to whether information collected by "cookies" are to be considered as personal information. "Cookies" do not independently identify a person. Cookies are placed by a web site on a particular visitor's computer in order for the web site to identify those same visitors when they return to the site. The data collected by the cookies relate more to the use of the computer itself rather than to the use by a particular person. That being said cookies can be linked with other data such as a registration form at the web site or can be profiled down to concern only one particular individual (the data can no longer be considered as anonymous because with a reasonable effort one can determine the individual user).

2.2 Controller

The directive provides for a number of duties and obligations incumbent on the « controller ». Furthermore the determination of the national law applicable depends on

the "establishment" of the controller[8]. One must therefore determine who can be considered as the controller in the CYBERBRAND project.

According to article 2.d of the directive, the controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Uncertainty still reigns over the exact powers and functions of each actor in the CYBERBRAND project. Several possibilities must be examined. The first possibility is to consider the consortium of companies which have developed CYBERBRAND are to be considered as controllers. They determine the purposes of the processing of the personal data (conception and development of data gathering in order to optimise and to customise the offer for each user) and to this effect determine the means of this processing (development of a software tool to this effect). However, the development of the software tool does not necessarily imply that the consortium actually processes the data. It does not exercise any factual control on the data. It should not therefore be qualified as the controller.

The second possibility is to consider the retailer as the controller. If the retailer determines jointly with the developer of the software, the means of the processing it is also he who determines the purpose of the processing and who actually possesses the data. The retailer processes the data for his own benefit and is the one who determines the outcome of the processing of the data. The retailer must therefore be considered as the controller of the data processing.

3 Principles to be respected

The directive and the German legislation lay down a series of principles that must be respected by the controller. We will examine each one of these principles underlying the main implications for the CYBERBRAND project.

[8] According to article 4.1.a the Member State must apply its law to the processing of personal data carried out in the context of activities of an establishment of the controller on the territory of the Member State.

3.1 The Purpose Limitation Principle

3.1.1 Personal data must be processed fairly and lawfully (article 6).

"Fair" processing implies a maximum of openness. An individual's personal data cannot be processed for any hidden or occult reasons. Personal data may only be collected in a transparent way (this principle is guaranteed by the right of information, granted to the data subject in articles 10 and 11).

"Lawful" processing implies the respect of the national provisions taken in compliance with Chapter II of the directive.

3.1.2 Personal data must be processed for specified, explicit and legitimate purposes

Personal data may only be processed for specified and explicit purposes. This obligation compels the controller to determine at the outcome of the processing, the exact purpose for which he intends to process personal data[9]. The determination of the purpose by the data controller must be sufficiently precise to enable the data subject to control every use of his personal data. For example, the purpose behind the CYBERBRAND project is not only the processing of personal data so as to establish personal profiles for retailers so that they can offer a personalised service, but also to optimise and customise the Website to meet customer preferences.

The purposes for which personal data are processed must be legitimate and must be determined at the time of collection of the data (article 6.1.b). One must therefore balance the right of the individual to see his right to privacy preserved with the public or private interest to process the data. The final evaluation of the legitimacy of the purposes depends on the appreciation of the courts or of specialised data protection authorities.

3) Personal data may not be further processed in a way incompatible with the purposes for which the data was collected

The fact that personal data may not be processed in a way "incompatible " with the purposes for which the data was initially collected, does not exclude the use of the data for secondary purposes, but does limit the extension of the use of the data. Since the directive aims at ensuring a maximum of openness with regard to the

[9] This obligation is further reflected in the data subject's right to be informed. See below.

data subject, any intended non-obvious purpose in relation with the purpose for which the data was initially collected could be regarded as "incompatible".

For example, as regards the services selling goods on Internet, customers will assume that the personal data that they may be requested to give to CONRAD when accessing the data base in order to purchase a good will be used only in order to deliver the goods and bill their purchase. The establishment of personal profiles of the clients to target the clientele will not necessarily be considered as an obvious use of his data by the data subject unless CONRAD has informed its clientele of this prior to the accessing of the database.

3.2 Grounds for processing of personal data

Article 7 of the Directive lays down the grounds justifying the processing of personal data. These grounds correspond to the circumstances considered by the European Community as allowing the processing of personal data. In order to be lawful, the processing of data must rely on one of these grounds, in addition to the fact that it must respect the obligations deriving from the legitimate purpose principle. Similarly in Germany the Teleservices Data Protection Act (TDDSG) provides that "personal data may be collected, processed and used by providers for performing teleservices only if permitted by this Act or some other regulation or if the user has given his consent"[10]. We will therefore also examine the purposes retained by the German TDDSG permitting the processing of personal data.

3.2.1 Article 7 of Directive

In the context of electronic commerce transactions, three justifications laid down in article 7 can more precisely be retained. One must examine for each one of these, whether or not they can justify the processing of personal data in the CYBERBRAND project:

i) "The data subject has unambiguously given his consent" (article 7.a):

Express written consent is not required. Any customer introducing his own personal data in order to purchase a good could be considered as consenting to the processing of his personal data for this specified purpose. The introduction of further data in order to obtain a personalised service could also be equated to the data subject giving his/her consent to the processing of the data by the retailer (Conrad, for example). However that does not necessarily imply that he accepts that a third party processes his data. If the data is to be transmitted to a third party,

[10] §3 of TDDSG

the data subject must consent specifically to the processing of his data by that third party.

Furthermore, if a user enters the website without necessarily going on to browse through the sites various pages, that does not necessarily imply that he consents to his data being processed for the purpose of the profiling of visitors to the website.

The data subject's consent must in any event be freely given[11]: there should be no pressure on the individual to obtain this consent. Free consent also implies that when a user is presented with a screen demanding personal data for further access, the fact that he refuses to go further should not be recorded or held against him.

The consent must also be informed, which means that vendors should inform each potential user of the service unequivocally about what he intends to do with the data and the risks this could incur for his privacy (see below, right to be informed). This enables the data subject to balance these risks against the expected benefits.

Lastly, the consent must be specific, it must relate to particular uses of the data for specified purposes. Any modification of the purpose that is incompatible with the initial purpose requires a new consent. For example, if the data subject introduces personal data in the context of goods offered by CONRAD, he does not necessarily consent to the transmission of his data third parties such as the CYBERBRAND consortium.

Similarly the access to a website does not imply the consent to the automatic creation and setting of a cookie on the users computer. In so far as cookies constitute personal data (see above), the consent to the cookies must be specific and fully informed.

ii) "Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (article 7.b).

Article 7.b implies not only that the processing corresponds to a pressing social or commercial need, but also that the processing is proportionate to the aim of the

[11] The data subject's consent is defined in article 2.h. of the Directive as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

contract[12]. The extent to which this provision can justify the profiling of the clientele or the analysis of visits to a web site is uncertain.

iii) "Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject..." (article 7.f).

This provision justifies the processing of personal data where it is in the legitimate interest of a natural or legal person, provided that the interests of the data subject are not overriding. This means that if the interest of a person in receiving personal data prevails over the data subject's interest not having his data communicated, data may be transferred. This is also true even when the data subject's interest in retaining his data is equivalent to the third party interest. It is only when the data subject's interest prevails, that the data relating to him may not be processed or communicated.

The provider may have an interest to store and process personal data relating to his customers and gathered from the visits to web sites or from the use of cookies so as to cultivate the supplier-customer relationship and to tailor his offer to the personal preferences of the customer. Additionally, there is an interest to optimise and customise the website to meet customer demands. On the other hand however, the customer has an interest in providing as little information as possible. A balance of interests must therefore be carried out as regards the processing of the data by the retailer[13]. Therefore if the collection and use of personal data by retailers might be seen as necessary in the interest of achieving the best possible conditions for product marketing; they may be outbalanced by the data subject's interest in maintaining his/her privacy. The strength of the data subject's interest will most probably increase according to the precision and sensitivity of the data processed.

[12] See on this subject « Privacy, Data Protection and Copyright : Their Interaction in the Context of Electronic Copyright Management Systems », op. cit., p.18.

[13] The directive leaves it up to the Member States to determine how the interests will be balanced.

3.2.2 Principles for the processing of personal data under the TDDSG

According to the TDDSG, personal data may be collected, processed and used by providers for performing of teleservices[14] only if permitted by the Act itself or some other regulation or if the user has given his consent. The provider may use the data collected for the performing of teleservices for other purposes only if permitted by the Act itself or by some other regulation or if the user has given his consent. The processing of data in the CYBERBRAND project does not fall within the scope of the definition of teleservices nor within the purposes permitted by the Act and the data subject's consent must therefore be obtained.

According to §3(6) of the TDDSG, before giving his consent the user must be informed of his right to withdraw his consent at any time with effect for the future. The consent can be declared electronically if the provider ensures that: such consent can be given only through an unambiguous and deliberate act by the user, consent cannot be modified without detection, the creator can be identified, the consent is recorded and the text of the consent can be obtained by the user on request at any time.

As concerns the processing and use of contractual data (data required for the concluding of a contract on the use of teleservices) for the purpose of advertising, market research or for the demand-oriented design of teleservices, §5 (2) provides that the consent must be explicitly given.

3.3 The Prohibition of Processing of Sensitive Data (article 8)

Subject to a number of exceptions set out in article 8.2, the processing of certain categories of data is prohibited according to article 8.1 of the directive. This prohibition covers any data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. Any messages or databases containing such data will therefore need to find grounds within article 8.2. in order to be processed.

[14] By « teleservices » the TDDSG includes : services offered in the field of individual communication (e.g. telebanking, data exchange) ; services offered for information or communication unless the emphasis is on editorial arrangement to form public opinion (data services providing e.g. traffic, weather, environmental and stock exchange data, the dissemination of information on goods and services) ; services providing access to the Internet or other networks ; services offering access to telegames ; goods and services offered and listed in electronically accesssible data bases with interactive access and the possibility for direct order (§2 (2)).

To the extent that profile information reveals an individual's morals as illustrated by an individual's consumer habits, such profiling comes within the ban of article 8.1. Similarly the electronic commerce activities linked to goods that reveal sensitive information fall within the scope of this article.

The data subject's explicit and informed consent is probably the safest course to follow when one decides to process sensitive data relating to an individual (article 8.2.a). The other most obviously eligible ground to process sensitive data is when such data have been manifestly made public by the data subject[15] (in answering a questionnaire he has marked his preference for gay activities, or his religion, for example).

3.4 Data Quality

Both the directive and the Teleservices Data Protection Act require a level of quality for the personal data that is being processed. The controller must ensure the respect of these principles.

1) Personal data must be adequate, relevant and not excessive in relation to the purposes for which they were collected and/or further processed.

The criteria of data adequacy are designed solely to ensure a necessary and sufficient link between the information and the purpose of the processing. For each finality, one must question whether or not there is a sufficient connection between the purpose and the data collected. Any irrelevant data must be discarded.

In the context of CYBERBRAND, the data collected must therefore always ensure a sufficient link with the purpose of offering a specially customer-tailored range of products, services and promotions. If the collection and use of data such as the customer's name, address, number of persons in their household, hobbies and preferences can be justified as offering a sufficient link with the service offered, this could not be said of data such as the person's passport number or place of birth.

It must be pointed out that the targeted marketing offered requires more information to be given prior to the offering of the service, than the traditional distance selling of goods. Indeed in order be able to offer the most personalised service possible, the vendor will require a number of data before the goods are actually proposed, so as to offer goods corresponding to the person's needs (age, hobbies,

[15] Article 8.2.e of the directive

sex...). The criteria of data adequacy could therefore enable the processing of more data than in a traditional environment.

The TDDSG also restricts the data that may be processed in the framework of teleservices. According to §3 (4) of the Act, "the design and selection of technical devices to be used for teleservices shall be oriented to the goal of collecting, processing and using either no personal data or as few as possible".

2) Personal data must be accurate and, where necessary, kept up to date.

An actor processing personal data must ensure that this data is accurate. The danger concerning the establishment of personal profiles based on consumer patterns is that the goods purchased may not necessarily correspond to a person's needs or habits: the purchase of a catholic bible does not mean that one is a catholic, one could be buying for someone else...It is recommended in this respect that the data subject is involved in the prior authorisation of the processing and that he is given the possibility to require that inaccurate data be modified (see below, right of rectification).

The personal data must be kept up to date. This implies that it be reviewed on a regular basis. Every reasonable step must be taken so that incomplete or inexact information is modified.

3) Personal data may only be kept for a certain period

Personal data may only be kept in a form which permits identification of the data subjects for no longer than is necessary for the purposes for which the data were collected and/or for which they are further processed. The data introduced by the consumer in order to purchase certain goods, may only be kept for the period necessary in order to obtain those goods and may not be stored beyond that period unless the controller has been specifically authorised to do so in the context of the profiling of his clientele.

One can question as to whether the vendor will be able to conserve data regarding individuals who enter the site but do not wish to go further and leave the site without having voluntarily entered personal data and without having purchased any goods.

The German TDDSG also provides that the personal data generated in connection with the process of requesting, accessing or otherwise using teleservices are

erased immediately upon conclusion if the procedure unless further storage is required for accounting purposes[16].

4 Rights of data subject

4.1 Right to be informed

According to article 10 and 11 of the directive, there are two particular occasions when the controller must provide information to the data subject. The first is at the time of collection of personal data. The data subject must be informed at least of:

a) the identity of the controller (and his representative, if any);

b) the purpose or purposes of the processing for which the data are intended.

Further information must also be provided if "necessary in the specific circumstances to ensure a fair processing in respect of the data subject". Such information includes: the recipients or categories of recipients of the data, whether replies to questions are obligatory or voluntary and the possible consequences of failure to reply, and the existence of the data subject's right of access to and the right to rectify the data concerning him.

If personal data on consumers are collected it must be clear to them who is to use the data and what are the purposes for which the data are to be used or disclosed.

It must be pointed out that the features of a network facilitate the provision of information. In the hypothesis of data collected from the data subject, a message can appear on the screen at the beginning of the operations, providing the users with the mandatory information.

The data subject must be informed of the identity of the recipients or categories of recipients. The "recipient" is defined in article 2.g. of the Directive as any person to whom the data are disclosed whether a processor (person processing data on behalf of the controller), third party (any person other than the data subject, the controller, the processor and persons who under the direct authority of the controller or processor, are authorised to process the data), a person in a third country... The controller may be requested to provide information as to the identity of these persons to the data subject if deemed necessary in order to guarantee "fair

[16] §4 (2) 2 of the TDDSG

processing" of the data. This will mean, for example, that Conrad will need to inform the data subject of the transmission of the data to any third party.

The text of the Directive does not provide any indication as to what particular circumstances justify additional information being given to guarantee a "fair processing" of the data in respect to the data subject. Articles 10 and 11 merely state that the additional information must be given "in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect to the data subject". The concept of "fair" processing, seems to refer to the requirement of transparency laid down in article 6.1.b. and in this respect one can consider that it is always recommended to give the data subject a maximum of information.

The second occasion when information must be provided to the data subject is where the data have not been directly obtained from the data subject. According to article 11, he must be informed at the time the data are recorded or, if a disclosure to a third party is envisaged, no later than at the time when the data are first disclosed. Extracted data can correspond to this type of data which is not directly obtained from the data subject but which is deduced from the combination of data.

The German TDDGS also provides that "the user shall be informed about the type, scope, place and purposes of collection, processing and use of his personal data". The provision then goes on to address the use of cookies stipulating that "in the case of automated processing which permits subsequent identification of the user and which prepares the collection, processing or use of personal data, the user shall be informed prior to the beginning of the procedure. The content of such information shall be accessible to the user at any time"[17]. Furthermore under §3(6) the user must be informed about his/her right to withdraw his/her consent to a data processing operation at any time. Finally §4(1) of the Act required that the user be notified of the options that exist for making anonymous or pseudonymous use and payment of teleservices.

It must be noted that article 11.2 provides for a derogation to the duty to inform the data subject where "in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort". This does not mean that the controller will not need to respect the principles laid down in the Directive (the purpose must be legitimate, the data must be relevant...). It does however mean that the control by the data subject of the use of his data will be considerably reduced. One must await the adoption of the relevant national legislation to determine the exact scope of the possible exceptions to the duty to inform the data

[17] §3(5) of TDDSG

subject, but it is probably correct to assume that the reference to "statistical purposes" implies that the data is anonymous.

4.2 Right of Access

The Directive grants every data subject the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay or expense, confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed.

The data subject may also obtain communication to him in an intelligible form of the data undergoing processing and any "available" information as to their sources. This could imply the obligation to reveal the sources of the information the controller has gathered on the web.

The German TDDSG also provides for the users right to information about data collected and stored concerning his person. Thus according to §7 he shall be entitled at any time and free of charge to inspect such data stored by the provider. If requested by the by the user, the information can be given electronically.

4.3 Right of rectification

Following on from the right of access, article 12. 2 of the directive provides that the data subject is granted, as appropriate, the right to obtain the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data. It is up to the controller to ensure that this right is guaranteed.

The Directive further provides that the controller must notify to the third parties to which the data have been disclosed of any rectification, erasure or blocking of the data, unless this proves impossible or involves a disproportionate effort. In the context of the sharing of information between the different actors, it is important that the notification of the rectification of the data is sent along to the different detainees of the data so that they may dispose of the most adequate and up dated information.

4.4 Right to Object

The data subject is granted the right to object on compelling legitimate grounds relating to his particular situation to the processing of data relating to him save where otherwise provided for by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve these data.

This right to object is granted unconditionally as regards the processing of personal data for marketing purposes. In the context of such projects as those developed by CYBERBRAND, therefore it would appear that this right must be granted.

Furthermore, when personal data are to be disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, the data subject must be informed of this before the data are disclosed and must be offered the right to object free of charge to such disclosures or uses. The sharing of information between actors so as to establish consumer profiles, thus requires the information of the data subject prior to the disclosure of the information.

Different ways of expressing ones right to opt out could be envisaged: by ticking the appropriate box when filling in a questionnaire collecting personal data; by writing; by e-mail or by telephone.

4.5 Automated individual decisions

Article 15 states that Member States shall grant the right to every person not to be subject to "a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct...»

This type of provision prevents decisions such as the creditworthiness of a person to be determined by an automated decision, based on the geographical localisation of the person, for example.

5 The controllers' obligations and liabilities

5.1.1 Security (article 17)

According to article 17 of the directive, the controller is required to put into place the measures so as to avoid any accidental or unlawful destruction, loss or alteration, against any unauthorised disclosure or access and against any other forms of unlawful processing[18]. The rationale of this article is that the potential danger to the data subject's right of privacy does not only emanate from the controller, who collects, stores, processes and discloses the data for his own purpose, but is also jeopardised if the data subject's data are misused by third parties who have gained access to it, whether authorised (by a processor under the instructions of the controller, for example) or unauthorised.

The security measures can be organisational (designation of a "security officer", documents handed out to the staff with precise security measures to be respected...) or technical (computers kept under lock and key or in specially protected areas, introduction of access codes, encryption of certain documents...). It is left up to the controller to adopt the necessary measures. The measures are the result of the equation of three variables: the risks of the processing, the nature of the data and the state of the art and cost of implementation of the measures.

The security measures adopted will also be dependent on the state of the art and the cost of their implementation. This provision implies that the controller is under the positive obligation to keep himself informed of the new security measures available and to ensure that the level of security is adequate vis a vis the "state of the art" unless they are prohibitively expensive. A controller could be well advised to have proof that all the decisions relating to security of personal data were founded on professional expertise.

The directive also provides that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical securities measures and organisational measures governing the processing to be carried out and must ensure compliance with these measures. The carrying out of processing of personal data by another person must be governed by a contract or legal act, in writing or in other equivalent form, binding the processor

[18] "Unlawful" processing covers any processing of personal data which does not respect the national provisions adopted in accordance with the Directive. This would be the case, for example, if a controller did not provide for instructions enabling his staff to process the data (see article 16). "Unauthorised" processing or destruction covers the cases when the controller does provide for such instructions, but staff process or intentionally destroy the data without the controller's permission. "Unauthorised" access covers the cases of interferences by third parties to data which they should not have access to.

to the controller and stipulating particularly that the processor shall only act on instructions from the controller and that the processor shall also be responsible for taking security measures in accordance with article 17 of the directive.

5.1.2 Notification (article 18)

The controller has a last obligation, which is that of notification of automated processing to a supervisory authority. The directive does however provide for the simplification or the exemption from notification for certain types of processing operations. It is not however clear how the national laws will transpose these measures. The general idea is to largely exempt controllers and to reserve the notification procedure for special categories of processing.

5.1.3 Liability (article 23)

The Directive provides every person with a right to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question. In addition, any person who has suffered a damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event-giving rise to the damage.

6 Conclusion

The CYBERBRAND project processes personal data according to the directive. In principle, the retailer (in this case CONRAD) rather than the consortium behind the development of the project must be qualified as the « controller ». The German Teleservices Data Protection Act will also apply if CONRAD can be considered as being established in Germany.

The controller must respect the following principles:

- **The purpose limitation principle**: personal data must be processed only for the explicit and specified purpose it was initially collected for (i.e. the sale of goods on

the Internet within the framework of a personalised service) and must not be processed in a way incompatible with those purposes.

- **Grounds for processing of personal data:** The data subject's consent is the safest ground to justify the processing of the data. The consent need not be written but it must be informed, specific and freely given.

- **Prohibition of processing of sensitive data:** It is recommended to obtain the data subject's explicit and informed consent before processing sensitive data (political opinions, ethnic origins, health, sex life, religious beliefs, trade-union membership).

- **Data Quality:** data must be adequate, relevant and non-excessive in relation to the purpose for which they were collected. There must be a sufficient link between the data and the purpose of the processing. Data must also be accurate and kept up to date.

The data subject has the following rights:

- **Right to be informed:** the data subject must know who is to use the data and what are the purposes the data will be used for or disclosed.

- **Right of access:** the data subject has the right to know whether personal data is being processed by the retailer and must be able to obtain communication of this data and « available » information as to their sources.

- **Right of rectification:** the data subject must be able to correct incomplete or incorrect information regarding him/her.

- **Right to object:** the data subject must be able to opt out or to refuse the processing of the data processed for direct marketing.

- **Right not to be subject to automated individual decisions:** the data subject must not be subject to an individual decision which produces legal effects concerning him or which significantly affects him, based solely on automated processing of the data.

The controller has the following obligations and liabilities:

- **Security:** the data subject's right to privacy must be guaranteed by adequate security measures.

- **Notification:** the processing must be notified according to national legislation.

- **Liability:** every person has a right to a judicial remedy for any breach in the applicable rights regarding personal data processing.